Inteligencia artificial y el límite de la privacidad

José Miguel Hernández López
Coordinador de protección de datos y transparencia en la Consejería de Educación, Formación Profesional, Actividad Física y Deportes del Gobierno de Canarias

RESUMEN: Estudio de los límites legales a la inteligencia artificial derivados de la privacidad: los derechos a la intimidad, a la protección de datos personales y al respecto de la vida privada de las personas, en el contexto de la creciente digitalización y uso de las nuevas tecnologías en los servicios públicos.

Palabras clave: Inteligencia artificial, privacidad, Reglamento de inteligencia artificial, protección de datos, intimidad, respeto a la vida privada, administraciones públicas.

ABSTRACT: Study of the legal limits to artificial intelligence arising from privacy: the rights to privacy, the protection of personal data, and respect for people's private lives, in the context of increasing digitalization and the use of new technologies in public services.

Keywords: Artificial intelligence, privacy, Artificial Intelligence Act, data protection, intimacy, respect for private and family life, public administrations.

1. INTRODUCCIÓN

> «Para muchos, en el contexto tecnológico actual, la privacidad constituye un prejuicio del pasado, un elemento que solo forma parte retóricamente de los derechos fundamentales».

https://doi.org/10.36151/RCAP.6.11

> «La pérdida de la privacidad parece ser uno de los signos definitorios de nuestro tiempo. Está vinculada a una tecnología que, vorazmente, reclama unos datos que poco a poco después son mercantilizados».
>
> [Ferran SÁEZ MATEU, *La intimidad perdida*, Barcelona, Herder Editorial, 2024, pp. 16 y 149]

El debate entre lo público y lo privado ha existido desde la antigüedad, desde Grecia (Tucídides, 460 a. C-395 a. de C., en su *Historia de la guerra del Peloponeso*) y Roma (Marco Tulio Cicerón, en su «Discurso sobre la casa», 57 a. C.) a nuestros días, destacando la aparición del concepto moderno de privacidad, que es un producto cultural que nace a finales del siglo XIX.

Desde las primeras referencias históricas a la privacidad, en cualquiera de sus manifestaciones y denominaciones como valor de la vida humana que debe ser protegido, hasta la actualidad, su configuración jurídica ha sido objeto de transformaciones profundas. Lo significativo es que, pese a los cambios políticos, económicos y sociales y a todas las reformas profundas en su regulación, el valor de la privacidad se ha ido concretando en el reconocimiento de un conjunto de derechos: a la intimidad personal y familiar; a la inviolabilidad del domicilio; al secreto de las comunicaciones; a la protección de datos personales; al respecto a la vida privada y familiar; y a los derechos digitales de intimidad y protección de datos.

Con la IA nos encontramos ante una nueva era tecnológica, lo que obliga a reflexionar una vez más sobre estos derechos. La presencia de máquinas inteligentes se ha consolidado como una realidad habitual en la vida de millones de personas, transformando los ámbitos de trabajo, educación, ocio e investigación. Esta evolución plantea importantes desafíos éticos y legales que es necesario abordar. Son muchas, por tanto, las preguntas que debemos plantearnos: ¿existen límites legales al uso de la inteligencia artificial (en adelante, IA)?; ¿la privacidad es un límite a la IA?; ¿qué es la privacidad?; ¿podemos confiar en una IA sin limitaciones?

Para poder responder a estos interrogantes, no compartimos la idea de una desregularización de la IA que libere de obligaciones a los que disponen de información y poder, de manera que vacíen de contenido los derechos de las personas. No son correctas las posiciones de indiferencia o inhibición de los poderes públicos. Si se quiere tener el control de la IA deben aprobarse normas, instrucciones y protocolos que refuercen las garantías sobre su desarrollo y aplicación, especialmente en el ámbito de los servicios públicos, para hacer realidad precisamente uno de los objetivos del Reglamento de Inteligencia Artificial[1] (en

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

adelante, RIA), la adopción de una IA «centrada en el ser humano y fiable» (considerando 1, RIA).

La globalización impone nuevas estructuras de poder. Además de los Estados y las organizaciones supraestatales como la Unión Europea (en adelante, UE), nos encontramos con corporaciones tecnológicas multinacionales cuya actividad puede afectar —y afecta— a los derechos fundamentales y que, en consecuencia, deben ser objeto de regulación. Como ha señalado Peter G. Kirchschlänger, profesor de Ética y director del Instituto de Ética Social ISE de la Universidad de Lucerna, «dada la incapacidad de las grandes empresas tecnológicas para cumplir con normas éticas, es una locura esperar que se vigilen a sí mismas»[2]. Frente a la idea extendida de que establecer normas sobre la IA impide la innovación, creemos que las leyes protegen las libertades y derechos de las personas, permitiendo así innovar con seguridad y respeto a derechos y valores superiores.

Al estudiar el RIA, se comprueba que la UE tiene como objetivo garantizar que los sistemas de IA que se usen en el mercado de la Unión sean seguros y respeten la legislación vigente en materia de derechos fundamentales y valores (considerando 1, RIA). Y estos son límites que deben tenerse en cuenta en el uso de la IA, y sobre los que trataremos en este artículo: los derechos fundamentales y los valores de la UE, centrándonos en concreto en los derivados de la privacidad.

Precisamente, el capítulo II del RIA se dedica a las **prácticas de IA prohibidas**, que abarcan todos los sistemas de IA cuyo uso se considera inaceptables **por ser contrarios a los valores de la Unión o porque violan derechos fundamentales**. Las interdicciones engloban aquellas prácticas que tienen un gran potencial para manipular a las personas mediante técnicas subliminales que trascienden su consciencia o que aprovechan las limitaciones de grupos vulnerables concretos, como los menores o las personas con discapacidad, para alterar de manera sustancial su comportamiento de un modo que es probable que les provoque perjuicios físicos o psicológicos a sí mismos o a terceros.

El RIA se publicó en el *Diario Oficial de la Unión Europea* el 12 de julio de 2024. De acuerdo con su artículo 113, el RIA entró en vigor a los veinte días de su publicación en el *Diario Oficial de la Unión Europea*, el día 1 de agosto de 2024.

Aunque el reglamento es aplicable con carácter general a partir del día 2 de agosto de 2026, se establece una aplicación gradual para determinados capítulos y artículos (art. 113, RIA):

- Los capítulos I y II serán aplicables a partir del 2 de febrero de 2025.
- El capítulo III, sección 4; el capítulo V; el capítulo VII; el capítulo XII y el artículo 78 serán aplicables a partir del 2 de agosto de 2025, a excepción del artículo 101.
- El artículo 6, apartado 1, y las obligaciones correspondientes del RIA serán aplicables a partir del 2 de agosto de 2027.

[2] Peter G. KIRCHSCHLÄNGER, «¿A cuántos niños más tiene que matar la IA?», *NEGOCIOS*, domingo 1 de junio de 2025, p. 15. En este artículo, el profesor KIRCHSCHLÄNGER cita al premio nobel de Física y pionero de la IA, Geoffrey Hinton, con una reflexión que corrobora la necesidad de la regulación de la IA: «Lo único que puede obligar a esas grandes empresas a investigar más sobre seguridad es la regulación gubernamental» (Geoffrey Hinton).

Un documento de gran interés en la materia que estudiamos son las *Directrices éticas para una IA fiable*[3], elaboradas por el Grupo independiente de expertos de alto nivel sobre inteligencia artificial, creado por la Comisión Europea en junio de 2018. Las *Directrices éticas*, citadas en el RIA en los considerandos 7, 27, 161 y en el artículo 95, establecen un marco para conseguir una IA fiable partiendo de un enfoque basado en los derechos fundamentales —«como derechos morales y legales», se dice textualmente— y respaldada por cuatro principios éticos que deben cumplirse para garantizar una IA ética y robusta: I) respeto de la autonomía humana; II) prevención del daño; III) equidad; y IV) explicabilidad. En este documento se incluye la «gestión de la privacidad y de los datos» entre los requisitos de la IA fiable:

> «3. Gestión de la privacidad y de los datos
>
> **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.
>
> 72) Protección de la intimidad y de los datos. **Los sistemas de IA deben garantizar la protección de la intimidad y de los datos a lo largo de todo el ciclo de vida de un sistema**. Esto incluye la información inicialmente facilitada por el usuario, así como la información generada sobre el usuario en el contexto de su interacción con el sistema (por ejemplo, los productos que genere el sistema de AI para determinados usuarios o la respuesta de estos a determinadas recomendaciones). Los registros digitales del comportamiento humano pueden posibilitar que los sistemas de IA no solo infieran las preferencias de las personas, sino también su orientación sexual, edad, género u opiniones políticas y religiosas. Para permitir que los individuos confíen en el proceso de recopilación de datos, es preciso garantizar que la información recabada sobre ellos no se utilizará para discriminarlos de forma injusta o ilegal».

Algunos apartados de este artículo son reelaboración de materiales propios de mis dos últimos trabajos *¿Por qué debemos proteger la privacidad? Cronología, textos y notas sobre intimidad, vida privada y protección de datos* (JM Bosch, 2023) y *Reglamento de Inteligencia Artificial. Incluye introducción, notas, cronología, webgrafía, bibliografía e índice analítico* (JM Bosch, 2024), manteniendo así una continuidad por el estudio de la privacidad, en este caso aplicado a la inteligencia artificial. De forma más general, también guardan relación con el

---

[3] Publicadas el 8 de abril de 2019.
https://digital-strategy.ec.europa.eu/es/library/ethics-guidelines-trustworthy-ai

presente artículo las dos primeras obras que publiqué, *El derecho a la protección de datos personales en la doctrina del Tribunal Constitucional* (Aranzadi, 2013) y el *Código de Transparencia y derecho de acceso a la información pública* (tirant lo blanch, 2015).

En los últimos veinte años he trabajado en protección de datos, y desde el año 2013 también en transparencia, desde la administración pública. Pues bien, hoy en día ya se reciben consultas y casos sobre estas mismas materias en relación con la inteligencia artificial, las cuales han tenido un desarrollo significativo a raíz especialmente de la aprobación del RIA en el año 2024.

2. VALORES

> «La idea de dignidad humana, a la que se considera un valor que debe respetarse de manera inexcusable, puesto que la persona humana no tiene precio (Kant), es el fundamento de todos los otros valores morales propios de la condición humana y de los valores que sirven para fundamentar cada tipo de derechos humanos o universales (seguridad, autonomía, libertad e igualdad)».
>
> [Gregorio PECES-BARBA, *Educación para la Ciudadanía y Derechos Humanos*, Madrid, Espasa, 2007, p. 123]

> «La aportación más original de la Constitución española de 1978 es, sin duda, la incorporación del concepto de valores superiores del artículo 1.º-1».
>
> [Gregorio PECES-BARBA, *Los valores superiores*, Madrid, tecnos, 1984]

Los valores de la UE están recogidos en el artículo 2 del Tratado de la Unión Europea:

> «La Unión se fundamenta en los **valores de respeto de la dignidad humana, libertad, democracia, igualdad, Estado de Derecho y respeto de los derechos humanos, incluidos los derechos de las personas pertenecientes a minorías**. Estos valores son comunes a los Estados miembros en una sociedad caracterizada por el pluralismo, la no discriminación, la tolerancia, la justicia, la solidaridad y la igualdad entre mujeres y hombres».

En el mismo sentido se expresa la Carta de los Derechos Fundamentales de la Unión Europea, al afirmar que «la Unión está fundada sobre los valores indivisibles y universales de la dignidad humana, la libertad, la igualdad y la solidaridad, y se basa en los principios de la democracia y el Estado de Derecho» (preámbulo de la Carta).

A fin de velar por el respeto de estos valores, el artículo 7 del Tratado de la Unión Europea prevé un mecanismo de la Unión para determinar la existencia, y la posible sanción, de una violación grave y persistente de los valores de la Unión recogidos en el artículo 2 por parte de un Estado miembro.

> «Artículo 7 del Tratado de la Unión Europea:
>
> 1. A propuesta motivada de un tercio de los Estados miembros, del Parlamento Europeo o de la Comisión, el Consejo, por mayoría de cuatro quintos de sus miembros y previa aprobación del Parlamento Europeo, **podrá constatar la existencia de un riesgo claro de violación grave por parte de un Estado miembro de los valores contemplados en el artículo** 2. Antes de proceder a esta constatación, el Consejo oirá al Estado miembro de que se trate y por el mismo procedimiento podrá dirigirle recomendaciones.
>
> El Consejo comprobará de manera periódica si los motivos que han llevado a tal constatación siguen siendo válidos.
>
> 2. El Consejo Europeo, por unanimidad y a propuesta de un tercio de los Estados miembros o de la Comisión y previa aprobación del Parlamento Europeo, **podrá constatar la existencia de una violación grave y persistente por parte de un Estado miembro de los valores contemplados en el artículo 2** tras invitar al Estado miembro de que se trate a que presente sus observaciones.
>
> (…)»

Pues bien, entre los valores de la UE se encuentra la privacidad, a la que dedicaremos el apartado siguiente. Ya constataba este límite de la privacidad el *Libro blanco sobre la inteligencia artificial. Un enfoque europeo orientado a la excelencia y la confianza*, publicado en el año 2020 por la Comisión Europea, donde se afirmaba lo siguiente:

> «Teniendo en cuenta el enorme impacto que puede tener la inteligencia artificial en nuestra sociedad y la necesidad de que suscite confianza, **resulta clave que la inteligencia artificial europea se asiente en nuestros valores y derechos fundamentales, como la dignidad humana y la protección de la privacidad**»[4].

A su vez, la Constitución española (en adelante, CE) incorpora los valores superiores de su ordenamiento jurídico en el artículo 1.1: la libertad, la justicia, la igualdad y el pluralismo político. Como ha señalado el profesor Peces Barba, los valores superiores tienen carácter normativo y «representan los ideales que una comunidad decide erigir como sus máximos objetivos a desarrollar por el ordenamiento jurídico»[5].

Por su parte, el RIA tiene entre sus fundamentos a los valores de la UE. De hecho, se hace referencia expresa a estos valores en los considerandos 1; 2; 6; 8; 27; 28; 31; 110; y en el artículo 40.3. En definitiva, el RIA busca promover una IA centrada en el ser humano y fiable, de conformidad con los valores de la UE.

---

4 https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52020DC0065

5 Véase Gregorio PECES BARBA, *Los valores jurídicos*, Madrid, Tecnos, 1984, p 42.

3. LA PRIVACIDAD COMO VALOR

> «Therefore, privacy has a social value. Even when it protects the individual, it does so for the sake of society».
>
> «Por lo tanto, la privacidad tiene un valor social. Incluso cuando protege al individuo, lo hace por el bien de la sociedad».
>
> [Daniel SOLOVE, «The meaning and value of privacy», en *Social Dimensions of Privacy*, Cambridge University Press, julio 2015, pp.71-82]

La privacidad es un valor que fomenta la autonomía y el desarrollo personal. Representa un objetivo, un ideal a conseguir por la sociedad. Se concreta en derechos, pero también se constituye como expresión de la moralidad mayoritariamente aceptada en un momento cultural e histórico determinado. La privacidad como valor tiene un doble contenido: jurídico y moral.

La privacidad es un valor jurídico, fundamento último de la positivización de derechos fundamentales como la intimidad o la protección de datos personales. Está en su fundamento y orígenes. Este valor jurídico busca el reconocimiento de derechos.

Pero el valor privacidad no se perfecciona exclusivamente con el reconocimiento de los derechos, ya que tiene también un contenido moral que realiza una función crítica y de presión social sobre los derechos a la privacidad ya positivizados, en aras de su concreción y de su profundización. Y requiere igualmente la aprobación de nuevos derechos. En esta materia la fuerza del cambio es formidable, dadas las transformaciones tecnológicas de la sociedad actual, donde los avances técnicos van acompañados de nuevos riesgos. De hecho, ya hay propuestas para la creación de derechos digitales con rango constitucional. En este sentido, en el preámbulo de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDPyGDD), se defiende la necesidad de «elevar a rango constitucional una nueva generación de derechos digitales».

El fundamento de este valor 'privacidad' es racional e histórico. Se plasma en reconocimientos legales, pero también en el consenso social. El sentido último del valor 'privacidad' surge de la reflexión racional y de la tradición histórica que terminan por concretarse en las sociedades democráticas.

El consenso de la privacidad lo podemos apreciar en distintos planos. En el ámbito internacional, en las declaraciones de derechos, destacando la Declaración Universal de los Derechos Humanos o el Convenio Europeo de los Derechos Humanos. Pero son muchas más las cartas o declaraciones donde se muestra este consenso[6]. En el ámbito nacional, el consenso se constata en la

---

[6] Véanse los siguientes ejemplos:
• *Declaración Europea sobre los Derechos y Principios Digitales para la Década Digital*, (2023/C 23/01).

Constitución, en su artículo 18, o con la aprobación de la LOPDPyGDD y de la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen. También en la jurisprudencia constitucional.

Pero no solo debemos destacar las declaraciones como muestra del consenso, también son muy relevantes las reflexiones de numerosísimos autores que nos acreditan la necesidad de protección de la privacidad en sus distintas dimensiones (desde Marco Tulio Cicerón a John Locke; Immanuel Kant; Benjamín Constant; Stuart Mill; Aldous Huxley; George Orwell; Hannah Arendt; Isaiah Berlin o Shoshana Zuboff[7]). Pero no solo se avanza con el consenso, también debemos de progresar aprendiendo de los conflictos: desde los casos históricos de Semayne (1604); Wilkes (1763); Gee v. Pritchard (1818); Olmstead v. United States (1928); Katz v. United States (1967); hasta los más recientes, como el caso Snowden[8] (2013), por el cual los periódicos *The Guardian* y *The Washington Post* recibieron el premio Pulitzer de periodismo por sus informaciones sobre el espionaje y vigilancia masiva de Estados Unidos, a raíz de las revelaciones de Edward Snowden. Otro caso muy relevante fue el de *Google Spain* S.L contra la Agencia Española de Protección de Datos (2014), sobre el derecho al olvido. También hay que destacar el caso *Cambridge Analytica*, cuando el 17 de marzo de 2018 los diarios *The New York Times*, *The Guardian* y *The Observer* denunciaron que *Cambridge Analytica* estaba explotando la información personal de los usuarios de Facebook, dando lugar a un uso indebido de los datos de millones de usuarios de esta red social. Probablemente uno de los casos más graves —con ruina económica, cárcel y suicidios de muchos de sus afectados—, es el de la oficina postal británica (1999-2025), que puede ser considerado uno de los mayores errores judiciales de la historia del Reino Unido, donde los acusados lucharon por defender su inocencia frente a una tecnología, en teoría infalible, pero defectuosa en la realidad[9].

Como valor, la privacidad nunca será plena, tiene una configuración siempre en desarrollo que busca el reconocimiento legal y a la vez su crítica para seguir avanzando.

---

https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32023C0123(01)

• *Recomendación sobre la Ética de la Inteligencia Artificial,* UNESCO (2021). https://www.unesco.org/es/articles/recomendacion-sobre-la-etica-de-la-inteligencia-artificial

• *Principios actualizados sobre la privacidad y la protección de datos personales,* Organización de Estados Americanos (2021). https://www.oas.org/es/sla/cji/docs/Publicacion_Proteccion_Datos_Personales_Principios_Actualizados_2021.pdf

7 Hemos dejado constancia de las reflexiones de numerosísimos autores en nuestra obra *¿Por qué debemos proteger la privacidad? Cronología, textos y notas sobre intimidad, vida privada y protección de datos*, Barcelona, editorial JM Bosch, 2023.

8 Véase la película *Snowen* (EE. UU., 2016), dirigida por Oliver STONE.

9 Véase la serie de cuatro capítulos *Mr. Bates contra correos* (Reino Unido, 2024), dirigida por James STRONG.

La privacidad está vinculada al valor superior de la libertad y a la dignidad de las personas. Ha sido reconocida entre los valores de la UE en el artículo 2, mediante la inclusión de los Derechos Humanos como uno de los valores fundantes de la UE. En este sentido, hay que subrayar que el artículo 12 de la Declaración Universal de los Derechos Humanos reconoce que «**nadie será objeto de injerencias arbitrarias en su vida privada**, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación (…)». En todo caso, las normas que reconocen los valores, como el artículo 2 del Tratado de la Unión Europea o el propio artículo 1.1 de la CE, no pueden ser cerradas. Como moralidad que son los valores, están abiertos a desarrollos no positivizados. En este sentido, consideramos que la privacidad ya forma parte de los valores de una sociedad democrática avanzada. La historia de la privacidad está directamente relacionada con el valor superior de la libertad y con la dignidad. Pero, llegados a este punto de desarrollo, en una sociedad en plena transformación digital, la privacidad es también un valor en sí mismo, sin olvidarnos de sus relaciones y vínculos con otros valores superiores del ordenamiento.

Al considerar a la privacidad como un valor jurídico se facilita la interpretación integradora entre los distintos derechos que la conforman. Es una guía para la interpretación y desarrollo de los derechos a la privacidad.

La existencia de valores que se positivizan en el ordenamiento jurídico ya no es algo excepcional. Los tribunales constitucionales de Alemania y España han subrayado en su doctrina jurisprudencial el vínculo entre valores y derechos fundamentales. Así, el Tribunal Constitucional Federal de Alemania ha entendido y estructurado los derechos fundamentales no sólo como derechos de defensa subjetivos del ciudadano frente al poder público, sino, además, como un orden de valores objetivo: «**en las disposiciones de derechos fundamentales de la Ley Fundamental se incorpora también un orden de valores objetivo**» (Sentencia BVerfGE 7, 198 (Lüth)).

El Tribunal Constitucional de España ha señalado que «no cabe desconocer, sin embargo, que **los derechos fundamentales responden a un sistema de valores** y principios de alcance universal que subyacen a la Declaración Universal y a los diversos convenios internacionales sobre Derechos Humanos, ratificados por España, y que, asumidos como decisión constitucional básica, han de informar todo nuestro ordenamiento jurídico» (Sentencia del Tribunal Constitucional 21/1981). Y ha calificado a la propia Constitución como un orden de valores que han de ponerse en conexión con la dignidad de la persona.

Como vemos, sin valores no hay derechos y sin derechos no hay democracia. En definitiva, consideramos a la privacidad como un valor que favorece la autonomía y el desarrollo integral de las personas y no como un derecho en sí misma. Se concreta este valor en un conjunto de derechos a la privacidad (intimidad, respeto a la vida privada, protección de datos, …), y en varias dimensiones como bienes jurídicos a proteger (vida íntima, vida privada, datos personales, …).

Por tanto, la privacidad tiene una doble vertiente: ética, como valor que favorece la autonomía y el desarrollo integral de las personas, y jurídica, que exige la inserción de ese valor en normas de derecho positivo, que busca el reconocimiento, protección y garantía de ese valor.

4. DERECHOS FUNDAMENTALES

> «**Los derechos fundamentales a la intimidad y a la protección de los datos personales se han vuelto más importantes para la protección de la dignidad humana que nunca antes**. Dichos derechos están consagrados en los Tratados de la UE y en la Carta de Derechos Fundamentales de la UE. Permite a las personas físicas que desarrollen sus propias personalidades, lleven a cabo vidas independientes, innoven y ejerzan sus derechos y libertades. Los principios de protección de datos definidos en la Carta de la UE (necesidad, proporcionalidad, imparcialidad, minimización de los datos, limitación a una finalidad específica, consentimiento y transparencia) se aplican al tratamiento de datos en su integridad, tanto respecto a la recopilación como a su uso.
>
> **La tecnología no debe dictar los valores y los derechos** ni la relación entre ambos debería reducirse a una falsa dicotomía.
>
> En el entorno digital actual, no basta respetar la ley sino que **tenemos que considerar la dimensión ética del tratamiento de datos**».
>
> [Supervisor Europeo de Protección de Datos. Resumen ejecutivo del Dictamen no 4/2015 del Supervisor Europeo de Protección de Datos, «Hacia una nueva ética digital: Datos, dignidad y tecnología»][10]

La Carta de Derechos Fundamentales de la Unión Europea reconoce los derechos individuales, civiles, políticos, económicos y sociales de las personas en la UE. La Carta fue proclamada en Niza en diciembre de 2000 por las principales instituciones de la UE. Desde diciembre de 2009, con el Tratado de Lisboa, es jurídicamente vinculante y tiene el mismo valor que los tratados de la UE. Se aplica a todas las instituciones y organismos de la Unión, así como a los Estados miembros al aplicar el Derecho de la UE.

La Carta consta de un preámbulo y de 54 artículos, agrupados en siete capítulos dedicados a la dignidad (I); libertades (II); igualdad (III); solidaridad (IV); ciudadanía (V); justicia (VI) y disposiciones generales (VII).

Pues bien, en el capítulo II, referido a las libertades, se reconocen los derechos fundamentales del respeto a la vida privada y familiar (art. 7) y a la protec-

---

[10] El texto completo del Dictamen puede consultarse en el *Diario Oficial la Unión Europea* de 25.11.2015, 2015/C 392/08]
https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52015XX1125(01)&from=ES

ción de datos de carácter personal (art. 8), derechos autónomos derivados del valor privacidad.

> «Artículo 7
>
> Respeto de la vida privada y familiar
>
> Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones.
>
> Artículo 8
>
> Protección de datos de carácter personal
>
> 1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.
> 2. Estos datos 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. Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación.
> 3. El respeto de estas normas estará sujeto al control de una autoridad independiente».
>
> [Artículos 7 y 8 de la Carta de Derechos Fundamentales de la Unión Europea]

Pero no solo han de tenerse en cuenta los derechos fundamentales de la UE como límites a la IA. Igualmente son aplicables, y límites por tanto, los derechos fundamentales reconocidos en la CE. En concreto, y derivados de la privacidad, son límites los derechos reconocidos en el artículo 18 de nuestra carta magna.

> «Artículo 18
>
> 1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.
> 2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito.
> 3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.
> 4. **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**».
>
> [Artículo 18 de la Constitución española]

P. Ovidius Naso afirmaba en el año 12 d. de C. que «las leyes se han hecho para que el poderoso no lo pueda todo» («datae leges ne fortior omnia posset»)[11]. Llama

[11] P. OVIDIUS NASO, *Fasti* 3, 279. Los *Fasti* se publicaron en torno al año 12 d. C.

la atención que, dos milenios después, sea actual esta concepción de la 'ley' como límite del poder. En este sentido, hay que subrayar que el artículo 18.4 de la CE —del que deriva el derecho a la protección de datos personales en nuestra carta magna— establece precisamente 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». Esta visión de la 'ley' como límite al poder se encuentra en numerosos textos históricos, entre otros en el *Discurso sobre el origen y los fundamentos de la desigualdad entre los hombres*, de Jean-Jaques Rousseau, dirigido a la Academia de Dijon, en 1754: «Porque cualquiera que sea cual sea la constitución de un gobierno, si hay un hombre que no está sujeto a la ley, todos los demás están necesariamente sujetos a él», «(…) no tienen otros amos que las sabias leyes que ustedes mismos han hecho»[12]. También Benjamín Constant de Rebecque subraya esta perspectiva de la 'ley' en su *Discurso sobre la libertad de los antiguos comparada con la de los modernos*, pronunciado en el ateneo de París, en 1819: «Preguntaros en primer lugar, señores, lo que hoy un inglés, un francés, un habitante de los Estados Unidos de América, entienden por la palabra libertad. Para cada uno es el derecho a no estar sometido sino a las leyes, de no poder ser detenido, ni condenado a muerte, ni maltratado de ningún modo, por el efecto de la voluntad arbitraria de uno o varios individuos»[13].

La IA no debe ser una tecnología sin límites ni control. Debe desarrollarse conforme a los derechos fundamentales «para que el poderoso no lo pueda todo», en la acertada expresión de Ovidius Naso.

5. DERECHOS A LA PRIVACIDAD

> «(…) hasta el presente, las **fronteras de la privacidad** estaban defendidas por el tiempo y el espacio. El primero procuraba, con su transcurso, que se evanescieran los recuerdos de las actividades ajenas, impidiendo, así, la configuración de una historia lineal e ininterrumpida de la persona; el segundo, con la distancia que imponía, hasta hace poco difícilmente superable, impedía que tuviésemos conocimiento de los hechos que, protagonizados por los demás, hubieran tenido lugar lejos de donde nos hallábamos. El tiempo y el espacio operaban, así, como salvaguarda de la privacidad de la persona.

Tomamos la cita de la obra de HERRERO LLORENTE, *Diccionario de expresiones y frases latinas*, Editorial Gredos, Madrid, 1980, p. 65.

12 Jean-Jaques ROUSSEAU, *Discurso sobre el origen y los fundamentos de la desigualdad entre los hombres,* Escuela Superior de Administración Pública, Bogotá, [17541] 2023, pp. 10-11 y 18-19.

13 Óscar GODOY ARCAYA, «Selección de textos políticos de Benjamín Constant», en *Estudios Políticos,* n.º 59, Centro de Estudios Públicos, invierno 1995, p. 52. En esta selección de textos se reproduce el discurso íntegro de Benjamín CONSTANT DE REBECQUE, pronunciado en el ateneo de París, en 1819, titulado *Discurso sobre la libertad de los antiguos comparada con la de los modernos*.

> Uno y otro límite han desaparecido hoy: Las modernas técnicas de comunicación permiten salvar sin dificultades el espacio, y la informática posibilita almacenar todos los datos que se obtienen a través de las comunicaciones y acceder a ellos en apenas segundos, por distante que fuera el lugar donde transcurrieron los hechos, o remotos que fueran éstos.
>
> (…) **Se hace preciso, pues, delimitar una nueva frontera de la intimidad** y del honor una frontera que sustituyendo los límites antes definidos por el tiempo y el espacio, los proteja frente a la utilización mecanizada, ordenada y discriminada de los datos a ellos referentes; **una frontera, en suma, que garantice que un elemento objetivamente provechoso para la Humanidad no redunde en perjuicio para las personas**. La fijación de esa nueva frontera es el objetivo de la previsión contenida en el artículo 18.4 de la Constitución, y al cumplimiento de ese objetivo responde la presente Ley».
>
> [Extracto de la exposición de motivos de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (derogada)]

Podemos leer múltiples referencias a la privacidad en los documentos oficiales (*v. gr.* Propuesta de Reglamento sobre la privacidad y las comunicaciones electrónicas) o en las noticias (*v. gr.* «Los teléfonos móviles se convierten en el campo de juego del mundial de la privacidad», *CincoDías*, 22 de noviembre de 2022). La palabra 'privacidad' aparece con regularidad en conversaciones personales. En algunos contextos se utiliza como sinónimo de vida privada, en otros como intimidad, y en ocasiones como equivalente a la protección de datos. De hecho, si leemos el título oficial de la propuesta de Reglamento sobre la privacidad y las comunicaciones electrónicas, en el mismo título de la norma propuesta aparecen tres conceptos que no significan exactamente lo mismo y que tampoco se definen en el cuerpo del texto normativo: respeto de la vida privada, protección de datos y privacidad:

> «Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el respeto de la ***vida privada*** y la ***protección de los datos personales*** en el sector de las comunicaciones electrónicas y por el que se deroga la Directiva 2002/58/CE (Reglamento sobre la ***privacidad*** y las comunicaciones electrónicas)[14]».

A priori, no parece del todo claro determinar con precisión de qué hablamos cuando hablamos de privacidad, ni siquiera cuando se incluye en textos legales, que requerirían conceptos indubitados. Tampoco se encuentran definiciones claras y concluyentes de la privacidad en los diccionarios generales. De hecho, la palabra 'privacidad' ha sido incluida en el *Diccionario de la lengua española* de forma muy reciente, en su edición 21.ª, de 2001. En concreto, la segunda acepción de 'privacidad' significa «ámbito de la vida privada que se tiene derecho a proteger

---

14 https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52017PC0010

de cualquier intromisión», y el *Diccionario panhispánico de dudas* precisa: «no es sinónimo de intimidad ('ámbito íntimo, espiritual o físico, de una persona')», aunque ambos términos están semánticamente muy próximos y son intercambiables en algunos contextos. No es casualidad que Díaz Rojo en su artículo «Privacidad: ¿neologismo o barbarismo?»[15] nos diga que «el contenido semántico de privacidad constituye el principal problema lingüístico» referido a esta palabra.

Para intentar aclarar la cuestión, podemos diferenciar tres posibles criterios sobre la existencia de un derecho o de varios derechos a la privacidad, que vamos a denominar tesis unitaria, plural y mixta.

La tesis unitaria defendería la existencia de un derecho único a la privacidad, lo que permitiría una protección global y directa de toda ella, con la ventaja de no tener que ir creando nuevos derechos a medida que fueran apareciendo nuevos riesgos.

De acuerdo con la tesis plural, el ordenamiento jurídico reconoce un conjunto de derechos a la privacidad, entendida como dimensión del ser humano que debe ser objeto de protección. La privacidad, en definitiva, es un valor de la vida humana que debe ser protegido. Y para ello, el ordenamiento jurídico reconoce diferentes derechos que permiten su defensa, distinguiendo cada una de las manifestaciones de la privacidad que deben ser garantizadas. Ante el surgimiento de nuevos riesgos para los intereses y derechos de las personas que pusieran en peligro la privacidad, se podrían reconocer nuevos derechos. Pensemos en este sentido en el nacimiento, ya en el siglo XXI, del «derecho al olvido», un derecho que forma parte de la protección de datos y que hoy en día se regula en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos, en adelante, RGPD). En definitiva, la consideración de la privacidad como valor nos permite caracterizarla por su carácter integrador.

Tesis mixta, de acuerdo con la cual el ordenamiento jurídico combina ambos sistemas: sin perjuicio de regular varios derechos que afectan a la privacidad, como la intimidad o la protección de datos, se reconoce, o debe reconocerse, un derecho general de la privacidad.

Por nuestra parte, defendemos la tesis plural, dado que no hay reconocido en nuestro ordenamiento jurídico ningún derecho general a la privacidad y sí diferentes derechos que permiten su defensa, según la dimensión que se proteja en cada caso: vida íntima, datos personales, vida privada, inviolabilidad del domicilio o secreto de las comunicaciones. Esta concepción permite el tratamiento jurídico separado de cada una de las manifestaciones de la privacidad, al tener características propias, y que requieren diferente valoración y tutela, sin perjuicio de las relaciones y conexiones entre todos estos derechos. Esta

---

15 https://digital.csic.es/handle/10261/3662?locale=es

tesis tampoco limitaría el reconocimiento de nuevos derechos que afectaran a nuevas dimensiones de la privacidad que las transformaciones sociales hicieran necesario proteger.

Cuáles son estos derechos que configuran la privacidad como valor de la vida humana que debe ser protegido, y que se han ido configurando en distintos momentos históricos, hasta llegar al momento presente en que se reconocen en nuestro ordenamiento jurídico. Son los siguientes:

- Derecho a la intimidad personal y familiar
- Derecho al respecto a la vida privada y familiar
- Derecho a la protección de datos personales
- Derechos digitales de intimidad y protección de datos

A ellos se suman otros dos derechos que no son objeto de estudio en el presente artículo, pero que dejamos apuntados, el derecho a la inviolabilidad del domicilio y el derecho al secreto de las comunicaciones, reconocidos en el artículo 18, apartados 2 y 3, de la CE.

Como ya hemos señalado, no encontramos en nuestra legislación estatal ni en la comunitaria un derecho a la privacidad en sí mismo reconocido. Se recogen, eso sí, cada vez más referencias a la privacidad, pero siempre se terminan concretando en los derechos que anteriormente hemos señalado.

Describimos brevemente a continuación el contenido de los derechos a la intimidad personal y familiar; al respecto a la vida privada y familiar; a la protección de datos personales; y los derechos digitales de intimidad y de protección de datos, que configuran todos ellos la privacidad.

Derecho a la intimidad personal y familiar. 1. Derecho fundamental reconocido en el artículo 18.1 de la CE, que tiene por objeto disfrutar de un ámbito propio y reservado para desarrollar una vida personal y familiar plena y libre, excluido tanto del conocimiento como de las intromisiones de terceros. Deriva de la dignidad de la persona, elemento básico y preeminente del ordenamiento jurídico. 2. De acuerdo con el artículo 20.4 de la CE, también es un límite del derecho a la libertad de expresión e información. 3. Derecho concebido para servir a la humanidad. 4. Derecho de la personalidad.

Derecho al respeto a la vida privada. 1. Derecho reconocido en el artículo 8 del Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales y en el artículo 7 de la Carta de los Derechos Fundamentales de la Unión Europea, por el que se garantiza a toda persona un amplio espacio de respeto de su vida en el desarrollo de su existencia personal y de sus relaciones con su entorno más cercano. 2. Derecho concebido para servir a la humanidad. 3. Es un derecho de la personalidad.

Derecho de protección de datos personales. 1. Derecho fundamental por el que se garantiza a las personas físicas el control sobre sus datos de carácter personal, concebido para servir a la humanidad. Deriva del artículo 18.4 de la CE. 2. Se re-

conoce en el artículo 8.1 de la Carta de los derechos fundamentales de la Unión Europea y en el artículo 16.1 Tratado de Funcionamiento de la Unión Europea. Se regula en el RGPD. 3. Derecho concebido para servir a la humanidad.

Derechos digitales de intimidad y de protección de datos. Los derechos digitales son los derechos de los ciudadanos en el entorno digital, ya sean derechos fundamentales (garantizados en la CE con el máximo nivel de protección) o derechos ordinarios. Se regulan en el Título X de la LOPDPyGDD. Entre los derechos digitales se encuentran el derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral; el derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo o el derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral.

6. EL RESPETO A LA VIDA PRIVADA Y EL DERECHO A LA INTIMIDAD CÓMO LÍMITES

> «Así como vida pública y privada son términos relativos, relativos uno del otro, intimidad es un término absoluto. La vida privada es variable en cada cultura y según los momentos históricos. La intimidad está al margen de la dialéctica público-privado, pero a la vez está en la raíz de la posibilidad de las dos esferas y de su mutua dependencia. Sólo desde la intimidad puede haber vida privada y vida pública, y sólo desde el reconocimiento y protección de su valor absoluto pueden definirse los ámbitos de las otras dos esferas».
>
> [Norberto GONZÁLEZ GAITANO, *El deber de respeto a la intimidad*, Pamplona, Ediciones Universidad de Navarra, 1990, p. 44]
>
> «Lo privado se contrapone a lo público; lo íntimo, en cambio, a lo que no es compartible *ni puede ser compartido* sin que su sentido se desvirtúe de inmediato».
>
> [Ferran Sáez Mateu, *La intimidad perdida*, Barcelona, Herder Editorial, 2024, p. 34]

En el RIA publicado en español en el *Diario Oficial de la Unión Europea* se hace referencia al derecho a la intimidad en los considerandos 27; 28; 43; 57; 60; 67; 68; 69; 80 y 110; y en los artículos 2.7 y 10.5.b). Sin embargo, en la versión publicada en inglés se recoge este derecho como «the right to privacy», y en la versión en francés como «Le droit au respect de la vie privée» ¿Son los mismos derechos el derecho a la intimidad y el derecho al respeto de la vida privada?

Estamos realmente ante dos derechos autónomos, intimidad y respeto a la vida privada, directamente relacionados pero diferentes. La regulación del derecho a la intimidad se establece en el artículo 18.1 de la CE y el derecho al respeto de la vida privada se reconoce en los artículos 7 de la Carta de Derechos Fundamentales de la Unión Europea y 8 del Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales (CEDH, 1950). No obstante, hemos de recordar que el derecho a la vida privada ya se consagra en el artículo 12 de la Declaración Universal de los Derechos Humanos (1948) al reconocer que «nadie será objeto de

injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques».

El concepto de vida privada y familiar es más extenso que el de intimidad y, en este sentido, el Tribunal Europeo de Derechos Humanos resalta con respecto al concepto de vida privada cuatro características esenciales: i) nos encontramos ante una noción amplia que no debe interpretarse restrictivamente; ii) no es susceptible de una definición exhaustiva; iii) debe analizarse caso a caso, conforme a las circunstancias del supuesto de hecho concreto; y iv) abarca múltiples elementos de la identidad física y social de un individuo.

Desde el punto de vista del Tribunal Europeo de Derechos Humanos, la vida privada no se circunscribe a la vida íntima, donde cada uno pudiera llevar su vida personal a su manera y descartar completamente el mundo de fuera de ese círculo. El respeto a la vida privada debe incluir, en cierta medida, el derecho de un individuo a entablar y desarrollar relaciones con sus semejantes y, por lo tanto, puede extenderse a las actividades profesionales y comerciales.

A diferencia de esta interpretación expansiva del Tribunal Europeo de Derechos Humanos en relación con el derecho al respeto de la vida familiar, el Tribunal Constitucional de España ha realizado una interpretación más restrictiva del derecho a la intimidad reconocido en el artículo 18.1 de la CE. En este sentido, afirma que «la garantía de la vida privada de la persona y de su reputación poseen hoy una dimensión positiva que excede el ámbito propio del derecho fundamental a la intimidad (art. 18.1 CE)» (STC 292/2000). La intimidad implica, como ha señalado el TC, «la existencia de un ámbito propio y reservado frente a la acción y conocimiento de los demás, necesario —según las pautas de nuestra cultura— para mantener una calidad mínima de la vida humana» (STC 231/1988).

El considerando 69 del RIA señala que «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» [«The right to privacy and to protection of personal data must be guaranteed throughout the entire lifecycle of the AI system»]. La interpretación que defendemos es que realmente el límite que establece el RIA para los sistemas de IA es el respeto a la vida privada, más amplio que el derecho a la intimidad, y debe tenerse así en cuenta al analizar e interpretar el RIA. Todo lo íntimo es privado, pero no todo lo privado es íntimo. Y debe protegerse ante los sistemas de IA tanto la intimidad como la vida privada, además de los datos personales amparados por el derecho a la protección de datos.

Por último, debemos de subrayar dos ideas extraídas del propio RIA en relación con el derecho a la intimidad —y también con el respeto a la vida privada, como hemos argumentado—, que actúan como límites:

- Los sistemas de IA empleados para controlar el rendimiento y el comportamiento de las personas en las relaciones contractuales de índole laboral

pueden socavar sus derechos fundamentales a la intimidad (considerando 57, RIA).

- El Derecho de la UE en materia de la intimidad y la confidencialidad de las comunicaciones se aplicará a los datos personales tratados en relación con los derechos y obligaciones establecidos en el RIA (artículo 2.7, RIA).

7. EL DERECHO DE PROTECCIÓN DE DATOS COMO LÍMITE

La protección de datos es un derecho fundamental por el que se garantiza a las personas físicas el control sobre sus datos de carácter personal, que además constituye un instituto de garantía de los derechos a la intimidad, al honor y del pleno disfrute de los restantes derechos fundamentales.

En este sentido, el considerando 1 del RGPD es concluyente al señalar la naturaleza de este derecho: «la protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental». Por su parte, el artículo 1.a), párrafo segundo, de la LOPDPyGDD tampoco deja lugar a dudas: «el derecho fundamental de las personas físicas a la protección de datos personales, amparado por el artículo 18.4 de la Constitución, se ejercerá con arreglo a lo establecido en el Reglamento (UE) 2016/679 y en esta ley orgánica».

El artículo 8.1 de la Carta de los Derechos Fundamentales de la Unión Europea también reconoce el derecho a la protección de datos: «toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan».

No obstante, también hay que subrayar que el derecho a la protección de datos no es ilimitado, como han declarado tanto el Tribunal Constitucional Federal alemán en su sentencia de 15 de diciembre de 1983 y como el Tribunal Constitucional español en su Sentencia 292/2000, fundamento jurídico 11. El propio RGPD, en su considerando 4, expresa con nitidez los límites de este derecho:

> «(…) El derecho a la protección de los datos personales no es un derecho absoluto sino que debe considerarse en relación con su función en la sociedad y mantener el equilibrio con otros derechos fundamentales, con arreglo al principio de proporcionalidad. El presente Reglamento respeta todos los derechos fundamentales y observa las libertades y los principios reconocidos en la Carta conforme se consagran en los Tratados, en particular el respeto de la vida privada y familiar, del domicilio y de las comunicaciones, la protección de los datos de carácter personal, la libertad de pensamiento, de conciencia y de religión, la libertad de expresión y de información, la libertad de empresa, el derecho a la tutela judicial efectiva y a un juicio justo, y la diversidad cultural, religiosa y lingüística».
>
> [Considerando 4, RGPD]

Igualmente es importante destacar que la protección de datos, además de ser un derecho fundamental, es un instituto de garantía de las libertades públicas y

de los derechos fundamentales de las personas físicas, como ha señalado el Tribunal Constitucional en reiteradas sentencias: «(…) instituto de garantía como forma de respuesta a una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona, pero que es también en sí mismo un derecho o libertad fundamental» (Sentencia del Tribunal Constitucional 254/1993); «(…) este precepto [18.4 Constitución española] contiene un instituto de garantía de los derechos a la intimidad y al honor y del pleno disfrute de los restantes derechos ciudadanos que es, además, en sí mismo un derecho fundamental» (Sentencia del Tribunal Constitucional 290/2000, fundamento jurídico 7).

Como límite a la IA, hay que subrayar los siguientes puntos referidos a la protección de datos que extraemos del propio RIA:

- Las normas que establece el RIA deben entenderse sin perjuicio del Derecho vigente de la UE, en particular en materia de protección de datos (considerando 9, RIA).
- Las normas armonizadas para la introducción en el mercado, la puesta en servicio y la utilización de sistemas de IA establecidas del RIA deben facilitar la aplicación efectiva y permitir el ejercicio de los derechos en materia de protección de datos personales (considerando 10, RIA).
- Los sistemas de IA empleados para controlar el rendimiento y el comportamiento de estas personas también pueden socavar sus derechos fundamentales a la protección de los datos personales (considerando 57, RIA).
- El derecho a la protección de datos personales debe garantizarse a lo largo de todo el ciclo de vida del sistema de IA (considerando 69, RIA).
- El RIA se entiende sin perjuicio de las competencias, funciones, poderes e independencia de las autoridades de protección de datos (considerando 157, RIA).

8. ADMINISTRACIONES PÚBLICAS E INTELIGENCIA ARTIFICIAL

> «Ya hay oficinas locales donde los empleados cargan a ChatGPT expedientes con datos personales de los ciudadanos sin anonimizar la información y sin ser conscientes de que la IA puede empezar a tomar decisiones a partir de criterios desconocidos para los funcionarios.
>
> (…)
>
> No se trata solo de lo que la IA puede hacer, sino de lo que debemos permitirle hacer».
>
> [«Un poder invisible que debe regularse», editorial *EL PAÍS*, lunes 28 de julio de 2025, p. 12][16]

[16] La noticia que tiene como fundamento la opinión de esta editorial se publicaba el mismo día en el periódico: «En algunos municipios se usa ChatGPT sin control», *EL PAÍS*, lunes 28 de

La IA está transformando la manera en que las administraciones públicas (en adelante, AAPP) gestionan la información y los datos, por lo que deben implementarse medidas para garantizar la protección de los datos personales, la transparencia, la supervisión humana y el propio cumplimiento del RIA.

8.1. Cumplimiento en protección de datos

Es aplicable el RGPD y la LOPDPyGDD cuando se haga uso de datos personales en actuaciones administrativas afectadas por la IA. En estos casos, habrán de cumplirse, entre otros, los siguientes puntos:

- Identificar con precisión las finalidades y la base jurídica de los tratamientos (arts. 5 y 6, RGPD).
- Establecer mecanismos visibles, accesibles y sencillos, incluidos los medios electrónicos, para el ejercicio de derechos (art. 12, RGPD).
- El derecho a la protección de datos personales es un derecho de derechos, que podrán ejercer las personas afectadas por sistemas de IA. Es un derecho fundamental en sí mismo (art. 18.4, CE) y además lo configuran un conjunto de derechos, como son los derechos de acceso; de rectificación; de oposición; de supresión; al olvido; a la limitación del tratamiento, de portabilidad; y de no ser objeto de decisiones individualizadas (capítulo III, RGPD).

  En relación con la IA hay que destacar el derecho del interesado a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte de significativamente de modo similar (art. 22, RGPD)[17].
- Informar a los interesados conforme a los artículos 12, 13 y 14 del RGPD. Deberá informarse de forma concisa, inteligible, de fácil acceso y con un lenguaje claro y sencillo, sobre la naturaleza de los sistemas de IA que emplean, qué algoritmos utilizan, la finalidad del sistema y el tipo de datos procesados.
- Realizar un análisis de riesgo para los derechos y libertades de los ciudadanos de todos los tratamientos de datos que desarrollen sistemas de IA que afecten a datos personales (art. 24, RGPD).

---

julio de 2025, p. 28. La noticia la encabezaba la siguiente afirmación: «Alimentar con datos de los ciudadanos los modelos de lenguaje tiene riesgos como ceder soberanía e incurrir en discriminación».

17 Sobre el derecho del interesado a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, véase la Sentencia del Tribunal de Justicia de la Unión Europea (Sala Primera), de 7 de diciembre de 2023. https://curia.europa.eu/juris/document/document.jsf;jsessionid=32730EC98571CACB1615E-69882702DEE?text=&docid=280426&pageIndex=0&doclang=ES&mode=req&dir=&occ=first&part=1&cid=489949

- En el caso de que existan encargados del tratamiento ha de garantizarse que ofrezcan garantías suficientes para aplicar medidas técnicas y organizativas apropiadas (art. 28, RGPD).
- Revisar las medidas de seguridad que se aplican a los tratamientos a la luz de los resultados del análisis de riesgos (disposición adicional primera de la LOPDPyGDD).
- Establecer mecanismos para identificar con rapidez la existencia de violaciones de seguridad de los datos y reaccionar ante ellas
- Valorar si los tratamientos que se realizan requieren una Evaluación de Impacto sobre la Protección de Datos cuando impliquen un alto riesgo para los derechos y libertades de los interesados (art. 35, RGPD).
- Designar delegados de protección de datos (art. 34, LOPDPyGDD).

8.2. Cumplimiento en transparencia

Las AAPP que utilicen sistemas de IA, especialmente aquellos clasificados como de alto riesgo, estarán obligadas a garantizar la publicidad activa y el derecho de acceso a la información pública:

- Publicidad activa.
  - Publicar la relación de procedimientos que incluyan el uso de la IA.
  - Registro público de los sistemas de IA de alto riesgo.
- Garantizar el derecho de acceso a la información pública referente a los procedimientos donde se incorpora el uso de la IA.

En relación con el denominado *principio de transparencia algorítmica*, que impone a las AAPP obligaciones de información de las características esenciales de los algoritmos empleados en la toma de decisiones, es de especial interés la Sentencia del Tribunal Supremo, Sala de lo Contencioso-Administrativo, Sección Tercera, núm. 1119/2025, de 11 de septiembre de 2025, donde declara:

> «1. El derecho de acceso a la información pública trasciende a su condición de principio objetivo rector de la actuación de las Administraciones públicas, para constituir un derecho constitucional ejercitable, como derecho subjetivo, frente a las Administraciones públicas, derivado de exigencias de democracia y transparencia, e inseparablemente unido al Estado democrático y de Derecho.
>
> 2. **El derecho de acceso a la información pública adquiere especial relevancia ante los riesgos que entraña el uso de las nuevas tecnologías en el ejercicio de las potestades públicas o la prestación de servicios públicos,** como ocurre con el empleo de sistemas informáticos de toma de decisiones automatizadas en la actividad de las Administraciones públicas, especialmente, cuando tienen por objeto el reconocimiento de derechos sociales. **En estos casos debe conllevar exigencias de transparencia de los procesos**

informáticos seguidos en dichas actuaciones, con el objeto de proporcionar a los ciudadanos la información necesaria para su comprensión y el conocimiento de su funcionamiento, lo que puede requerir, en ocasiones, el acceso a su código fuente, a fin de posibilitar la comprobación de la conformidad del sistema algorítmico con las previsiones normativas que debe aplicar».

[Sentencia del Tribunal Supremo, Sala de lo Contencioso-Administrativo, Sección Tercera, núm. 1119/2025, de 11 de septiembre de 2025, Fundamento de Derecho Noveno]

También es relevante destacar en esta materia la regulación establecida en el artículo 23 de la Ley 15/2022, de 12 de julio, integral para la igualdad de trato y la no discriminación, a la que precisamente hace referencia en sus fundamentos jurídicos la Sentencia del Tribunal Supremo de 11 de septiembre de 2025.

«Artículo 23. Inteligencia Artificial y mecanismos de toma de decisión automatizados.

1. En el marco de la Estrategia Nacional de Inteligencia Artificial, de la Carta de Derechos Digitales y de las iniciativas europeas en torno a la Inteligencia Artificial, **las administraciones públicas favorecerán la puesta en marcha de mecanismos para que los algoritmos involucrados en la toma de decisiones que se utilicen en las administraciones públicas tengan en cuenta criterios de minimización de sesgos, transparencia y rendición de cuentas, siempre que sea factible técnicamente**. En estos mecanismos se incluirán su diseño y datos de entrenamiento, y abordarán su potencial impacto discriminatorio. **Para lograr este fin, se promoverá la realización de evaluaciones de impacto que determinen el posible sesgo discriminatorio.**

2. Las administraciones públicas, en el marco de sus competencias en el ámbito de los algoritmos involucrados en procesos de toma de decisiones, priorizarán la transparencia en el diseño y la implementación y la capacidad de interpretación de las decisiones adoptadas por los mismos.

3**. Las administraciones públicas y las empresas promoverán el uso de una Inteligencia Artificial ética, confiable y respetuosa con los derechos fundamentales**, siguiendo especialmente las recomendaciones de la Unión Europea en este sentido.

4. Se promoverá un sello de calidad de los algoritmos».

[Artículo 23 de la Ley 15/2022, de 12 de julio, integral para la igualdad de trato y la no discriminación]

8.3. Cumplimiento del RIA

Enfoque basado en el riesgo (considerandos 26 y 27, RIA). Con el fin de establecer un conjunto proporcionado y eficaz de normas vinculantes, el RIA aplica

un enfoque basado en los riesgos, de forma tal que adapta el tipo y contenido de las normas a la intensidad y el alcance de los riesgos que se puedan generar. En coherencia con ello, prohíbe determinadas prácticas de inteligencia artificial que no son aceptables, define los requisitos que deben cumplir los sistemas de IA de alto riesgo y las obligaciones aplicables a los operadores pertinentes, así como impone obligaciones de transparencia.

Prácticas prohibidas. Los riesgos inaceptables determinan prácticas prohibidas, reguladas en el capítulo II del RIA. En concreto, la lista de prácticas de IA prohibidas está prevista en el artículo 5, y que podemos agrupar en los siguientes apartados[18]:

i) Técnicas manipuladoras subliminales y engañosas. Se prohíbe cualquier sistema de IA que utilice técnicas subliminales o manipuladoras con el objetivo de alterar significativamente el comportamiento de una persona o grupo, reduciendo su capacidad para tomar decisiones informadas, y que cause o pueda causar perjuicios considerables [art. 5.1.a), RIA].

ii) Explotación de vulnerabilidades. Está prohibido cualquier sistema de IA que aproveche las vulnerabilidades de personas debido a su edad, discapacidad, situación social o económica, con la finalidad de alterar su comportamiento de manera que cause perjuicios considerables [art. 5.1.b), RIA].

iii) Evaluación y clasificación social. No se permite la introducción, puesta en servicio o uso de sistemas de IA que clasifiquen a las personas basándose en su comportamiento social o características personales para generar puntuaciones ciudadanas que provoquen tratos perjudiciales o desfavorables, injustificados o desproporcionados [art. 5.1.c), RIA].

iv) Evaluación de riesgos de actividad delictiva. Prohibido el uso de IA para evaluar riesgos de que una persona cometa un delito basándose únicamente en la elaboración de perfiles o en características de personalidad, salvo si se apoya en la valoración humana basada en hechos objetivos y verificables [art. 5.1.d), RIA].

v) Creación de bases de datos de reconocimiento facial masivas. No se permite la introducción en el mercado, la puesta en servicio para este fin específico o el uso de sistemas de IA que creen o amplíen bases de datos de reconocimiento facial mediante la extracción no selectiva de imágenes faciales de internet o de circuitos cerrados de televisión [art. 5.1.e), RIA].

---

[18] Para conocer el concepto y significado de las prácticas prohibidas, es necesario, el estudio del artículo 5 del RIA y consultar los considerandos 3; 5; 26; 27; 28; 29; 30; 31; 32; 33; 34; 35; 36; 37; 38; 39; 40; 41; 42; 43; 44 y 45 RIA; y el anexo II, Sistemas de IA de alto riesgo a que se refiere el artículo 6, apartado 2, RIA.

vi) Inferencia de emociones en lugares de trabajo y centros educativos. Prohibido el uso de IA para inferir emociones en lugares de trabajo y centros educativos, excepto cuando se use por motivos médicos o de seguridad [art. 5.1.f), RIA].

vii) Categorización biométrica discriminatoria. No se permite la categorización de individuos basándose en datos biométricos para deducir raza, opiniones políticas, afiliación sindical, creencias religiosas o filosóficas, vida sexual u orientación sexual, salvo en el ámbito de la garantía del cumplimiento del Derecho [art. 5.1.g), RIA].

viii) Identificación biométrica remota en tiempo real. Prohibido el uso en espacios públicos con fines de garantía del cumplimiento del Derecho, salvo en casos específicos y estrictamente necesarios como la búsqueda de víctimas de delitos graves, prevención de amenazas a la vida o seguridad física, y localización de sospechosos de delitos graves [art. 5.1.h), RIA].

Sistemas de alto riesgo. Los sistemas de IA de alto riesgo, según el RIA, son aquellos que presentan un riesgo significativo para la salud, seguridad y derechos fundamentales de las personas (considerando 46, RIA). Se regulan en el capítulo III y en el anexo III. A fin de garantizar que los sistemas de IA de alto riesgo sean altamente fiables, debe someterse a dichos sistemas a una evaluación de la conformidad antes de su introducción en el mercado o puesta en servicio (considerando 123, RIA). Es precisamente en el anexo III donde encontramos las referencias a los servicios públicos esenciales (anexo III, apartado 5), entre otros servicios prestados por las AAPP como el de educación (anexo III, apartado 3).

Es importante reseñar que el hecho de que un sistema de IA sea clasificado como de alto riesgo por el RIA, NO implica que su uso sea legal. Habrá de cumplir la normativa de la UE y nacional, como por ejemplo en protección de datos, como establece con claridad meridiana el considerando 63 del RIA. El RIA no es fundamento jurídico legitimador para el tratamiento de datos personales, salvo que dispusiera específicamente otra cosa.

> «**El hecho de que un sistema de IA sea clasificado como un sistema de IA de alto riesgo en virtud del presente Reglamento no debe interpretarse como indicador de que su uso sea lícito** con arreglo a otros actos del Derecho de la Unión o del Derecho nacional compatible con el Derecho de la Unión, por ejemplo, en materia de protección de los datos personales o la utilización de polígrafos y herramientas similares u otros sistemas para detectar el estado emocional de las personas físicas. Todo uso de ese tipo debe seguir realizándose exclusivamente en consonancia con los requisitos oportunos derivados de la Carta y de los actos aplicables del Derecho derivado de la Unión y del Derecho nacional. **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, RIA]

Sistemas de alto riesgo en las AAPP. En aplicación del RIA, con carácter general, el uso de la IA por las AAPP en la prestación de servicios públicos ha de considerarse de alto riesgo, al impactar en derechos y deberes de los ciudadanos. Los sistemas de IA de alto riesgo, según el RIA, son aquellos que presentan un riesgo significativo para la salud, seguridad y derechos fundamentales de las personas (considerando 46, RIA). Se regulan en el capítulo III y en el anexo III.

Si examinamos el anexo III, establece un conjunto de usos en los que podemos identificar numerosos servicios prestados por las AAPP. Así el bloque 1 se dedica a la biometría, en la medida en que su uso esté permitido por el Derecho de la Unión o nacional aplicable; el bloque 2 incluye las **infraestructuras críticas**; el bloque 3, **educación y formación profesional**; el bloque 4, empleo, gestión de los trabajadores y acceso al autoempleo; el bloque 5, **el acceso** a servicios privados esenciales y **a servicios y prestaciones públicos esenciales y disfrute de estos servicios y prestaciones**; el bloque 6, garantía del cumplimiento del Derecho, en la medida en que su uso esté permitido por el Derecho de la Unión o nacional aplicable; el bloque 7, migración, asilo y gestión del control fronterizo, en la medida en que su uso esté permitido por el Derecho de la Unión o nacional aplicable; el bloque 8, administración de justicia y procesos democráticos.

Evaluación de impacto relativa a los derechos fundamentales para los sistemas de IA de alto riesgo (art. 27, RIA). Con el fin de garantizar eficazmente la protección de los derechos fundamentales, los **responsables del despliegue de sistemas de IA de alto riesgo que sean organismos de Derecho público**, o las entidades privadas que presten servicios públicos, deben llevar a cabo una evaluación de impacto relativa a los derechos fundamentales antes de su puesta en funcionamiento (art. 27, RIA).

- Objetivo de esta evaluación: que el responsable del despliegue determine los riesgos específicos para los derechos de las personas o colectivos de personas que probablemente se vean afectados y defina las medidas que deben adoptarse en caso de que se materialicen dichos riesgos.
- La evaluación de impacto debe llevarse a cabo antes del despliegue del sistema de IA de alto riesgo.
- Actualización. Debe actualizarse cuando el responsable del despliegue considere que alguno de los factores pertinentes ha cambiado.
- No son equivalentes las evaluaciones de impacto relativas a los derechos fundamentales para los sistemas de IA de alto riesgo (art. 27, RIA) y la relativa a la protección de datos (art. 35, RGPD). En todo caso podrán complementarse, como indica el artículo 27.4 del RIA.

Supervisión humana (art. 14, RIA). Los sistemas de IA de alto riesgo deben diseñarse y desarrollarse de tal modo que las personas físicas puedan supervisar su funcionamiento, así como asegurarse de que se usan según lo previsto y de que sus repercusiones se abordan a lo largo del ciclo de vida del sistema.

- También es esencial garantizar que los sistemas de IA de alto riesgo incluyan mecanismos destinados a orientar e informar a las personas físicas a las que se haya asignado la supervisión humana para que tomen decisiones con conocimiento de causa acerca de si intervenir, cuándo hacerlo y de qué manera, a fin de evitar consecuencias negativas o riesgos, o de detener el sistema si no funciona según lo previsto.
- **El objetivo de la supervisión humana será prevenir o reducir al mínimo los riesgos para la salud, la seguridad o los derechos fundamentales** que pueden surgir cuando se utiliza un sistema de IA de alto riesgo conforme a su finalidad prevista o cuando se le da un uso indebido razonablemente previsible, en particular cuando dichos riesgos persisten a pesar de la aplicación de otros requisitos establecidos en la presente sección.

Transparencia en el RIA. El considerando 27 del RIA nos indica lo que ha de entenderse por transparencia: «que los sistemas de IA se desarrollan y utilizan de un modo que permita una trazabilidad y explicabilidad adecuadas, y que, al mismo tiempo, haga que las personas sean conscientes de que se comunican o interactúan con un sistema de IA e informe debidamente a los responsables del despliegue acerca de las capacidades y limitaciones de dicho sistema de IA y a las personas afectadas acerca de sus derechos». El principio de transparencia tiene una regulación detallada en el RIA, al que se dedican el artículo 13, dentro del capítulo III, de sistemas IA de alto riesgo, sobre la transparencia y comunicación de información a los responsables del despliegue; el artículo 50, en el capítulo IV, de obligaciones de transparencia de los proveedores y responsables del despliegue de determinados sistemas de IA; y el anexo XII, referido a la información sobre transparencia a que se refiere el artículo 53, apartado 1, letra b) — documentación técnica de los proveedores de modelos de IA de uso general para los proveedores posteriores que integren el modelo en su sistema de IA.

¿Quién es quién en el RIA? El artículo 3 del RIA nos define los papeles de los distintos sujetos obligados, donde se prevé que las autoridades públicas puedan ser proveedores o responsables del despliegue[19]:

---

[19] Véase sobre las obligaciones de las AAPP según sean proveedores o responsables del despliegue el artículo de Agustí CERRILLO I MARTÍNEZ, «El impacto del Reglamento de Inteligencia Artificial en las Administraciones públicas», *Revista Jurídica de les Illes Balears (RJIB)*, núm. 26, pp. 93-98.
https://revistajuridicaib.tirant.com/index.php/rjib/article/view/6

- Proveedor: «una persona física o jurídica, **autoridad pública**, órgano u organismo que desarrolle un sistema de IA o un modelo de IA de uso general o para el que se desarrolle un sistema de IA o un modelo de IA de uso general y lo introduzca en el mercado o ponga en servicio el sistema de IA con su propio nombre o marca, previo pago o gratuitamente» (art. 3.3, RIA).
- Responsable del despliegue: «una persona física o jurídica, o **autoridad pública**, órgano u organismo que utilice un sistema de IA bajo su propia autoridad, salvo cuando su uso se enmarque en una actividad personal de carácter no profesional» (art. 3.4, RIA).
- Representante autorizado: «una persona física o jurídica ubicada o establecida en la Unión que haya recibido y aceptado el mandato por escrito de un proveedor de un sistema de IA o de un modelo de IA de uso general para cumplir las obligaciones y llevar a cabo los procedimientos establecidos en el presente Reglamento en representación de dicho proveedor» (art. 3.5, RIA).
- Importador: «una persona física o jurídica ubicada o establecida en la Unión que introduzca en el mercado un sistema de IA que lleve el nombre o la marca de una persona física o jurídica establecida en un tercer país» (art. 3.6, RIA).
- Distribuidor: «una persona física o jurídica que forme parte de la cadena de suministro, distinta del proveedor o el importador, que comercialice un sistema de IA en el mercado de la Unión» (art. 3.7, RIA).
- Operador: «un proveedor, fabricante del producto, responsable del despliegue, representante autorizado, importador o distribuidor» (art. 3.8, RIA).

Por todo ello:

- Las AAPP deben realizar evaluaciones previas a la decisión de implantar la IA que incluyan apartados específicos sobre el cumplimiento del RIA y de las normativas de protección de datos y transparencia.
- Como proveedoras y responsables del despliegue de la IA en los servicios públicos, las AAPP han de cumplir el RIA y las normativas de protección de datos y transparencia.

9. ¿SE HA DE RECONOCER UN NUEVO DERECHO PARA PROTEGERNOS FRENTE A LA INTELIGENCIA ARTIFICIAL?

> «(…) cuando el Derecho se enfrenta al problema práctico de definir un nuevo derecho que proteja al propio ser humano, en realidad se está enfrentando a un nuevo tipo de abuso».
>
> [María MARVÁN LABORDE, «Prólogo» a la obra de I. Davara Fernández De Marcos, *Hacia la estandarización de la protección de datos personales*, Madrid, La Ley, 2011, p. 20]

> «El problema más importante que se plantea a la especie humana y que la naturaleza obliga al hombre a resolver, es el de crear una sociedad civil que aplique el derecho de manera universal».
>
> [Immanuel KANT, *Idea para una historia universal en clave cosmopolita*, 1784]

Es una evidencia que la IA puede contribuir a generar beneficios económicos, como nuevos modelos de negocio de la economía digital, y producir avances de la investigación en las ciencias de la salud, por poner solo dos ejemplos de la relevancia que ya tiene en el desarrollo social. La IA puede ayudar —y así lo ha resaltado la Comisión europea en su comunicación «Inteligencia artificial para Europa»[20], de 30 de abril de 2018— por ejemplo, en el tratamiento de las enfermedades, en la reducción de las tasas de mortalidad en los accidentes de tráfico; en la lucha contra el cambio climático o en la previsión de las amenazas a la ciberseguridad. Pero también son constatables los riesgos reales de que la IA pueda utilizarse indebidamente y proporcionar instrumentos poderosos para llevar a cabo prácticas de manipulación y control social. Entre los grandes peligros de la IA se encuentra el sesgo algorítmico, ya que los sistemas de IA se entrenan en conjuntos de datos que pueden reflejar y amplificar los sesgos existentes en la sociedad, con las consecuencias de que conduzcan a la adopción de decisiones discriminatorias[21].

La principal crítica que debemos hacer al RIA es la falta de reconocimiento de un nuevo derecho específico frente a los abusos de la IA. El RIA parte de la premisa de que los derechos reconocidos en nuestro ordenamiento ya nos amparan frente a las malas prácticas en IA. En este sentido, no es casualidad que en el RIA se haga referencia en noventa y siete ocasiones a los derechos fundamentales. El considerando 9 del RIA es clarificador en cuanto a su concepción sobre la protección de los derechos, al establecer que las normas armonizadas que se establecen en el reglamento deben entenderse «sin perjuicio del Derecho vigente de la Unión, en particular en materia de protección de datos, protección de los consumidores, derechos fundamentales, empleo, protección de los trabajadores y seguridad de los productos, al que complementa el presente Reglamento» y que «en consecuencia, permanecen inalterados y siguen siendo plenamente aplicables todos los derechos y vías de recurso que el citado Derecho de la Unión otorga a los consumidores y demás personas que puedan verse afectados negativamente por los sistemas de IA».

---

20 https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52018DC0237

21 Véanse por su gran interés los riesgos que las propias empresas de IA, gobiernos y expertos han señalado, y que se referencian en las notas 1, 2, 3, 4, 5, 6, 7, 8 y 9 de la carta pública, de 4 de junio de 2024, de empleados de empresas de inteligencia artificial de vanguardia, en el que reclaman «A Right to Warn about Advanced Artificial Intelligence». https://righttowarn.ai/

Es cierto que los derechos fundamentales nos amparan, pero consideramos que no de una forma plena contra las nuevas formas de injusticia. Estimamos que debió darse un paso más, y ante una nueva realidad debía de haberse definido un derecho específico frente a la IA.

Marván Laborde señala de forma clarividente que «(…) cuando el Derecho se enfrenta al problema práctico de definir un nuevo derecho que proteja al propio ser humano, en realidad se está enfrentando a un nuevo tipo de abuso». Y esa es la realidad: nos estamos enfrentando ante novísimas formas de arbitrariedad que requieren sistemas de salvaguarda actualizados. La aprobación del RIA era el momento, y la norma apropiada, para instituir un nuevo derecho. Aunque la aprobación del reglamento es en sí mismo un acierto, adolece de este aspecto que estimamos esencial: la configuración de un derecho específico ante la IA.

La Carta de Derechos Digitales[22], publicada en julio de 2021, y que no tiene carácter normativo, ya apunta como hoja de ruta para futuros proyectos legislativos al reconocimiento de los «Derechos ante la Inteligencia Artificial»:

> «XXV. Derechos ante la inteligencia artificial
>
> 1. La inteligencia artificial deberá asegurar un enfoque centrado en la persona y su inalienable dignidad, perseguirá el bien común y asegurará cumplir con el principio de no maleficencia.
> 2. En el desarrollo y ciclo de vida de los sistemas de inteligencia artificial:
>
> a) Se deberá garantizar el **derecho a la no discriminación cualquiera que fuera su origen, causa o naturaleza, en relación con las decisiones, uso de datos y procesos basados en inteligencia artificial**.
>
> b) Se establecerán condiciones de transparencia, auditabilidad, explicabilidad, trazabilidad, supervisión humana y gobernanza. En todo caso, la información facilitada deberá ser accesible y comprensible.
>
> c) Deberán garantizarse la accesibilidad, usabilidad y fiabilidad.
>
> 3. **Las personas tienen derecho a solicitar una supervisión e intervención humana y a impugnar las decisiones automatizadas tomadas por sistemas de inteligencia artificial que produzcan efectos en su esfera personal y patrimonial**».

La Declaración Europea sobre los Derechos y Principios Digitales[23] para la Década también hace referencia la necesidad de dar poderes a las personas ante la IA Digital:

> «CAPÍTULO III. Libertad de elección
>
> Interacciones con algoritmos y sistemas de inteligencia artificial

---

22 https://www.lamoncloa.gob.es/presidente/actividades/Documents/2021/140721-Carta_Derechos_Digitales_RedEs.pdf

23 https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32023C0123(01)

…

9. **Toda persona debería estar empoderada** para beneficiarse de las ventajas de los sistemas algorítmicos y de inteligencia artificial, especialmente a fin de tomar sus propias decisiones en el entorno digital con conocimiento de causa, así como estar protegida frente a los riesgos y daños a su salud, su seguridad y sus derechos fundamentales».

Igualmente, la Oficina de Política Científica y Tecnológica (OSTP) de la Casa Blanca propuso en octubre de 2022 una Declaración de Derechos sobre Inteligencia Artificial (*AI Bill of Rights*)[24].

El RIA consta de ciento ochenta considerandos; trece capítulos; ciento trece artículos y trece anexos. Es la sección cuarta, del capítulo IX, la que se dedica a las vías de recurso y donde se regulan el derecho a presentar una reclamación ante una autoridad de vigilancia del mercado (art. 85); el derecho a explicación de decisiones tomadas individualmente (art. 86) y la denuncia de infracciones y protección de los denunciantes (art. 87). Como podemos comprobar, no hay un reconocimiento de un derecho específico que nos proteja de los abusos de la IA, dada la premisa de la que parte la norma: los derechos ya establecidos en el ordenamiento jurídico nos protegen plenamente frente a los sistemas de IA.

Una muestra de la necesidad de generar nuevos derechos para hacer frente a la realidad la encontramos en los derechos digitales, que se regulan en el Título X de la LOPDPyGDD. En el preámbulo de esa ley orgánica se dice expresamente que «una deseable futura reforma de la Constitución debería incluir entre sus prioridades la actualización de la Constitución a la era digital y, específicamente, elevar a rango constitucional una nueva generación de derechos digitales».

Es evidente que un número creciente de personas desarrolla una proporción significativa de su actividad laboral y personal en entornos digitales. Por tanto, hay una necesidad ineludible de proteger los derechos de las personas en el entorno digital, donde desarrollan gran parte de su vida personal y profesional. Uno de los desafíos de la legislación y la jurisprudencia en materia de IA estará en cómo se resuelvan las relaciones cada vez más complejas entre el Derecho y la tecnología.

¿Es necesario entonces reconocer un nuevo derecho para protegernos ante los sistemas de IA? Así lo creemos. La evolución jurídica de los derechos no está conclusa. Las declaraciones de los derechos que nos amparan y su configuración, y especialmente en el caso de los derechos fundamentales, nunca será una obra acabada. Es una labor en evolución y siempre lo será. Muestra de ello la tenemos en la configuración jurídica del derecho a la protección de datos a través de las sentencias del Tribunal Constitucional Federal Alemán, de 15 de diciem-

---

[24] https://www.managementsolutions.com/es/publicaciones-y-eventos/apuntes-normativos/notas-tecnicas-normativas/declaracion-de-derechos-sobre-inteligencia-artificial-ai

bre de 1983; del Tribunal Europeo de Derechos Humanos, de 26 marzo 1987, caso Leander contra Suecia; o del Tribunal Constitucional español 292/2000, de 30 de noviembre de 2000. Otro ejemplo, lo encontramos en la configuración del «derecho al olvido» por la Sentencia del Tribunal de Justicia de la UE, de 13 de mayo de 2014, o la garantía de los derechos digitales en el año 2018 por la LOPDPyGDD. Son ejemplos de cómo el Derecho se adapta a los cambios. La formación histórica de los derechos —fundamentales o de configuración legal— continúa. Por ello, se requiere i) ampliar los mecanismos de protección de los derechos ya reconocidos para que puedan ser aplicables en el ámbito digital y ii) declarar nuevos derechos específicos para este entorno, como sería el **derecho al control humano ante la IA**[25], con contenidos de no discriminación, supervisión e impugnación frente a los sistemas de IA.

Los cambios tecnológicos y, en definitiva, la realidad social habrán de determinar igualmente que las estructuras dogmáticas de derechos reconocidos, como la protección de datos, intimidad o el respeto a la vida privada, continúen evolucionando para dar una respuesta óptima a los nuevos problemas que se plantean. La formación histórica de los derechos es imparable. Los consensos y los conflictos habrán de impulsar que los derechos reconocidos se refuercen.

Son miles de millones los datos, textos e imágenes que están siendo generados por algoritmos. Una de sus consecuencias es que las personas están perdiendo el control de la información: no conocen bien qué datos se está operando por la IA, quién los trata, para qué se tratan y cómo se tratan; y, lo que es peor, tampoco saben que lo desconocen. Si la humanidad quiere tener el control de la IA, es imprescindible reconocer nuevos derechos y reforzar los existentes, ante la nueva realidad de transformación digital de nuestra sociedad.

A finales del siglo XIX, Samuel Warren y Louis Brandeis ya nos indicaron en su artículo «The Right to Privacy» (1890) que «la protección de la sociedad debe venir, principalmente, del reconocimiento de los derechos de la persona»[26]. No podemos olvidar su reflexión, debiendo esforzarnos como sociedad en disponer

---

25 Es cierto que el RIA dedica el artículo 14 a la supervisión humana, pero no se configura como un derecho en sí mismo, sino como un requisito de los sistemas IA de alto riesgo. El artículo 14 del RIA forma parte del capítulo III, sistemas de IA de alto riesgo, y dentro de él se regula en la sección 2, titulada «requisitos de los sistemas de IA de alto riesgo». Y no es equivalente ni tiene la misma trascendencia jurídica establecer la supervisión humana como un requisito que haberla reconocido como un derecho específico, con todas las garantías para las personas físicas que considerasen conculcado su derecho.
«**Deben aplicarse a los sistemas de IA de alto riesgo requisitos** referentes a la gestión de riesgos, la calidad y la pertinencia de los conjuntos de datos utilizados, la documentación técnica y la conservación de registros, la transparencia y la comunicación de información a los responsables del despliegue, **la supervisión humana**, la solidez, la precisión y la ciberseguridad (…)» (considerando 66, RIA).

26 Samuel WARREN y Louis BRANDEIS: *El derecho a la intimidad*, edición a cargo de Benigno Pendás, con traducción de Pilar Baselga, Madrid, Civitas, 1995, p. 72.

de herramientas jurídicas que nos permitan defendernos ante la creación de una IA sin control que todo lo domine.

La aprobación del RIA ha de valorarse como un acierto de la UE, que ha sabido prever los riesgos que puede implicar para los derechos y libertades fundamentales un mal uso de la IA. Empero, no es suficiente con concretar prohibiciones o preceptuar la realización de evaluaciones de impacto, como bien hace el RIA, entre numerosas medidas que reglamenta. Es necesario, igualmente, el reconocimiento de un derecho específico que nos proteja ante los abusos de la IA y un esfuerzo educativo que permita transmitir el respeto a los derechos fundamentales y tomar conciencia de lo que pueden implicar usos arbitrarios y sin control de la IA. El sistema educativo ha de garantizar la inserción del alumnado en la sociedad digital, de la que la IA va a tener cada vez mayor relevancia; pero las competencias digitales deben ir unidas al aprendizaje de un uso respetuoso de la IA con la dignidad humana y los valores de la UE. Con ello se daría cumplimiento a lo que proclama la Declaración Universal de los Derechos Humanos «como ideal común por el que todos los pueblos y naciones deben esforzarse, a fin de que tanto los individuos como las instituciones, inspirándose constantemente en ella, promuevan, mediante la enseñanza y la educación, el respeto a estos derechos y libertades».

La inteligencia artificial debe servir a la humanidad. Los avances en el ámbito de las tecnologías —no olvidemos que «la IA es un conjunto de tecnologías» (considerando 4, RIA)— afectan a la vida de las personas y han de analizarse, en consecuencia, en el contexto de las relaciones entre la ética, el derecho, la tecnología y el poder.

Es necesario contribuir al esfuerzo por dar a conocer la regulación de la IA, fomentar su uso respetuoso con los derechos fundamentales y reflexionar sobre la necesidad de reconocer un Derecho universal de control ante la IA para evitar su deshumanización.

10. EPÍLOGO

> «**El RIA no es la mejor ley posible, pero es una ley de primera generación**. Incluso las primeras leyes de protección de datos estaban muy lejos del RGPD. Esto es normal en la regulación tecnológica, el cruce entre interés económico, innovación y protección de los derechos exige compromisos».
>
> [Alessandro MANTELERO, «El Reglamento de inteligencia artificial: la respuesta del legislador europeo a los retos de la inteligencia artificial», en Lorenzo COTINO HUESO y Pere SIMÓN CASTELLANO, Pere (directores), *Tratado sobre el Reglamento de inteligencia artificial de la Unión Europea*, Aranzadi, 2024, p. 66]

- La utilización de sistemas de IA en la UE han de realizarse de conformidad con los valores y derechos fundamentales.

- Sin valores no hay derechos y sin derechos es imposible que exista democracia.
- La privacidad es un valor jurídico, fundamento último de la positivización de derechos fundamentales como el respeto a la vida privada, la intimidad o la protección de datos personales.
- La privacidad tiene una doble vertiente: ética, como valor que favorece la autonomía y el desarrollo integral de las personas; y jurídica, que exige la inserción de ese valor en normas de derecho positivo, que busca la protección y garantía de ese valor mediante el reconocimiento de derechos.
- Derechos a la privacidad. El valor de la privacidad se ha ido concretando históricamente en el reconocimiento de un conjunto de derechos fundamentales, entre los que se encuentran el derecho a la intimidad, la protección de datos personales y el respeto a la vida privada y familiar.
- Los derechos a la privacidad no son derechos absolutos. Están limitados por los restantes derechos fundamentales y por otros bienes y valores jurídicos igualmente reconocidos y protegidos.
- La estructura dogmática de los derechos a la privacidad y, con ella, su evolución jurídica, no está plenamente conclusa. La formación histórica de los derechos a la privacidad continúa.
- Sin garantizar los derechos al respeto a la vida privada y familiar, a la intimidad y a la protección de datos la privacidad no será posible. No obstante, el reconocimiento de estos derechos no será suficiente para protegernos de nuevos riesgos en una sociedad democrática en plena transformación digital. Es necesario realizar un esfuerzo pedagógico para divulgar en los distintos niveles educativos los derechos a la privacidad. Con ello se daría cumplimiento a lo que proclama el preámbulo de la Declaración Universal de los Derechos Humanos «como ideal común por el que todos los pueblos y naciones deben esforzarse, a fin de que tanto los individuos como las instituciones, inspirándose constantemente en ella, promuevan, mediante la enseñanza y la educación, el respeto a estos derechos y libertades».
- Es necesario garantizar un uso de la tecnología respetuoso con la dignidad humana y los derechos fundamentales, evitando la creación de un 'Gran hermano global' que todo lo controle y vigile.
- Las AAPP deben realizar evaluaciones previas a la decisión de implantar la IA que incluyan apartados específicos sobre el cumplimiento del RIA y de las normativas de protección de datos y transparencia.
- Las AAPP han de cumplir el RIA y las normativas de protección de datos y transparencia como proveedoras y responsables del despliegue de la IA en los servicios públicos.
- Los derechos al respeto a la vida privada y familiar, a la intimidad y a la protección de datos personales deben garantizarse a lo largo de todo el ciclo de vida de los sistemas de IA.

11. BIBLIOGRAFÍA GENERAL

BARRIO ANDRÉS, Moisés (director): *Comentarios al Reglamento Europeo de Inteligencia Artificial*, Madrid, LA LEY, 2024.

— *Manual de Derecho Digital*, 4.ª edición, Valencia, tirant lo blanch, 2025.

CAMPOS ACUÑA, M.ª Concepción (directora): *Kit básico para la implantación de la Inteligencia Artificial en el Sector Público*, Aranzadi LA LEY, EL CONSULTOR DE LOS AYUNTAMIENTOS, 2025.

CARLÓN RUIZ, Matilde: *Las administraciones públicas ante la inteligencia artificial*, Valencia, tirant lo blanch, 2025.

CERRILLO I MARTÍNEZ, Agustí; DI LASCIO; Francesca; MARTÍN DELGADO, Isaac y VELASCO RICO, Clara I. (directores); *Inteligencia artificial y Administraciones Públicas: una triple visión en clave comparada*, Madrid, Iustel, 2024.

COTINO HUESO, Lorenzo y SIMÓN CASTELLANO, Pere (directores): *Tratado sobre el Reglamento de inteligencia artificial de la Unión Europea*, Madrid, Aranzadi, 2024.

FEBLES POZO, Nayiber y NIETO ROJAS, Patricia (directores): *Inteligencia artificial y protección de datos: desafíos en la era digital*, A Coruña, Colex, 2025.

GAMERO CASADO, Eduardo (director) y PÉREZ GUERRERO, Francisco L. (coordinador): *Inteligencia artificial y sector público. Retos, límites y medios*, tirant lo blanch, 2023.

HERNÁNDEZ LÓPEZ, José Miguel: *¿Por qué debemos proteger la privacidad? Cronología, textos y notas sobre intimidad, vida privada y protección de datos,* Barcelona, editorial JM Bosch, 2023.

— *Reglamento de Inteligencia Artificial. Incluye introducción, notas, cronología, webgrafía, bibliografía e índice analítico*, Barcelona, editorial JM Bosch, 2024.

PECES BARBA, Gregorio, *Los valores superiores*, Madrid, Tecnos, 1984.

— *Lecciones de derechos fundamentales,* Madrid, Dykinson, 2004.

REBOLLO DELGADO, Lucrecio: *Inteligencia Artificial y Derechos fundamentales*, Madrid, Editorial Dykinson, 2023.

VESTRI, Gabrieli (director) y CAMPOS ACUÑA (coordinadora): *Inteligencia artificial en el sector público. Retos pendientes*, Madrid, LA LEY, EL CONSULTOR DE LOS AYUNTAMIENTOS, 2024.