PRIVACIDAD Y PROTECCIÓN DE DATOS EN LA ERA DIGITAL: RETOS Y OPORTUNIDADES DE LA CIBERSEGURIDAD

Teresa Aznar Montesino-Espartero

Curso 2025-2026

Grado en Derecho E-1, Universidad Pontificia de Comillas - ICADE

Tutor: Luis Bueno Ochoa

LISTADO DE PALABRAS CLAVE:

- AEPD: Agencia Española de Protección de Datos
- CE: Constitución Española
- CDFUE: Carta de los Derechos Fundamentales de la Unión Europea
- CEDH: Convenio Europeo de Derechos Humanos
- ENS: Esquema Nacional de Seguridad
- GDPR: General Data Protection Regulation
- IA: Inteligencia Artificial
- LOPDGDD: Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales
- NIS2: Directiva (UE) 2022/2555 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad
- RGPD: Reglamento General de Protección de Datos
- TEDH: Tribunal Europeo de Derechos Humanos
- TFUE: Tratado de Funcionamiento de la Unión Europea
- TJUE: Tribunal de Justicia de la Unión Europea
- UE: Unión Europea

RESUMEN

La digitalización de la sociedad ha transformado profundamente la forma en que se recopilan, almacenan y utilizan los datos personales. Este fenómeno ha convertido la privacidad y la protección de datos en elementos esenciales para la garantía de los derechos fundamentales de los ciudadanos. El presente trabajo analiza la evolución del derecho a la privacidad desde sus fundamentos filosóficos y jurídicos hasta su actual configuración como derecho fundamental autónomo. Asimismo, examina el marco normativo europeo y español en materia de protección de datos y ciberseguridad, prestando especial atención al Reglamento General de Protección de Datos (RGPD), la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD), la Directiva NIS2 y el Esquema Nacional de Seguridad.

Del mismo modo, se estudia la importancia de la ciberseguridad como instrumento indispensable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales frente a amenazas cada vez más complejas. Finalmente, se analizan los desafíos planteados por las nuevas tecnologías, especialmente la inteligencia artificial, poniendo de manifiesto la necesidad de compatibilizar la innovación tecnológica con la protección efectiva de los derechos fundamentales en el entorno digital.

Palabras clave: privacidad, protección de datos personales, ciberseguridad, derechos fundamentales, RGPD, inteligencia artificial, brechas de seguridad, autodeterminación informativa.

ABSTRACT

The digitalization of society has profoundly transformed the way personal data is collected, stored, and processed. This phenomenon has made privacy and data protection essential elements for safeguarding individuals' fundamental rights. This dissertation examines the evolution of the right to privacy from its philosophical and legal foundations to its current

status as an autonomous fundamental right. It also analyses the European and Spanish legal framework on data protection and cybersecurity, with particular attention to the General Data Protection Regulation (GDPR), the Spanish Organic Law on Data Protection and Digital Rights (LOPDGDD), the NIS2 Directive, and the National Security Framework.

Furthermore, the study explores the role of cybersecurity as a key mechanism for ensuring the confidentiality, integrity, and availability of personal data against increasingly sophisticated threats. Finally, it addresses the challenges posed by emerging technologies, particularly artificial intelligence, highlighting the need to balance technological innovation with the effective protection of fundamental rights in the digital environment.

Keywords: privacy, personal data protection, cybersecurity, fundamental rights, GDPR, artificial intelligence, data breaches, informational self-determination.

INTRODUCCIÓN

Estamos viviendo en un momento histórico, sin precedentes en la producción, circulación y explotación de los datos personales. La cantidad de datos que cada persona deja de forma consciente o inconsciente a través de sus aparatos digitales, de sus navegaciones por la red y de sus interacciones con servicios públicos y privados, ha alcanzado cifras que habrían parecido inimaginables hace apenas dos décadas. Este fenómeno, al que algunos han dado en llamar "economía del dato", ha llevado a situar la protección del ámbito privado de las personas en el centro de los debates jurídicos, políticos y éticos de nuestro tiempo.[1]

La privacidad en su dimensión contemporánea no es ya sólo el antiguo derecho a que nadie entre en la esfera íntima del individuo. Ha evolucionado hasta ser entendida como el poder de control que cada persona tiene sobre la información que le concierne, un poder que le permite, en última instancia, construir su propia identidad y participar en la vida social y

[1]Casas Baamonde, M. E. (coord.), *El derecho a la protección de datos personales en la sociedad digital*, Fundación Ramón Areces, Madrid, 2020, p. 11 (disponible en https://www.fundacionareces.es/recursos/doc/portal/2018/03/20/el-derecho-a-la-proteccion-de-datos-personales.pdf; última consulta: 2 de junio de 2026).

política en condiciones de igualdad y libertad. En la legislación española, ese poder encuentra su base constitucional en el artículo 18 de la Constitución de 1978, norma que, con una visión muy clara de futuro, ya previó en su cuarto apartado la tensión entre el uso de la informática y los derechos fundamentales de la persona.[2]

La respuesta normativa de la Unión Europea a este desafío se articula hoy principalmente a través del Reglamento (UE) 2016/679, conocido como Reglamento General de Protección de Datos (en adelante, RGPD), que desde su aplicación en mayo de 2018 ha supuesto una transformación radical tanto de la práctica empresarial como de la acción administrativa en todo el continente.[3] Sin embargo, la efectividad de ese marco normativo depende, en buena medida, de algo que ningún texto legal puede garantizar por sí solo: la existencia de medidas técnicas y organizativas capaces de preservar la integridad, confidencialidad y disponibilidad de los datos personales. A esta función responde la ciberseguridad, cuyo papel como garantía jurídica del derecho a la protección de datos constituye el hilo conductor del presente trabajo.

La elección de un tema no ha sido una decisión al azar. En los últimos años, las amenazas digitales se han multiplicado de manera exponencial. Las brechas de seguridad de grandes empresas, los ataques de ransomware a hospitales y administraciones públicas o la utilización masiva de datos personales con fines comerciales o políticos son, hoy, fenómenos cotidianos que afectan directamente al ejercicio de derechos fundamentales. Internet no conoce de barreras físicas o límites temporales lo que hace que cualquier vulneración de datos se convierta en un problema de alcance global.[4]

[2]Constitución Española, art. 18.4: «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».

[3]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 (Reglamento General de Protección de Datos), DOUE L 119, de 4 de mayo de 2016 (disponible en https://eur-lex.europa.eu/eli/reg/2016/679/oj?locale=es; última consulta: 2 de junio de 2026).

[4]Bouzas Mendes, R. E., «El reto de la privacidad en la era de internet», *Revista de Derecho UNED*, núm. 31, 2023, p. 113 (disponible en https://revistas.uned.es/index.php/RDUNED/article/view/37949/27892; última consulta: 2 de junio de 2026).

La metodología empleada es esencialmente jurídica: análisis de fuentes normativas primarias; Constitución española, RGPD, LOPDGDD, Directiva NIS2 y Esquema Nacional de Seguridad; estudio de la jurisprudencia relevante del Tribunal Constitucional, el Tribunal Europeo de Derechos Humanos (TEDH) y el Tribunal de Justicia de la Unión Europea (TJUE), y revisión crítica de la doctrina académica especializada. El trabajo se estructura en tres grandes partes que recorren el camino desde los fundamentos filosóficos hasta los retos más emergentes, pasando por el análisis del marco normativo vigente y el estudio de casos prácticos.[5]

PARTE I: FUNDAMENTOS FILOSÓFICOS Y JURÍDICOS

Capítulo 1. La privacidad como derecho fundamental

1.1. Fundamento filosófico: privacidad, dignidad y autonomía humana

La reflexión sobre la privacidad no nació en los despachos de abogados o en las empresas, sino en la filosofía política y moral que, desde la Ilustración, fue construyendo una teoría del sujeto autónomo capaz de autodeterminar su propia existencia al margen de las injerencias del poder político y social. La dignidad humana, en esta tradición, no es un atributo concedido por el ordenamiento jurídico, sino un presupuesto de este. El ser humano tiene dignidad que merece un espacio de libertad e intimidad inaccesible para terceros. En la terminología kantiana, la persona es siempre un fin en sí misma y nunca un mero instrumento, lo que implica, entre otras cosas, que nadie puede ser reducido a un conjunto de datos al servicio de intereses ajenos.[6]

[5]Polo Roca, A., «El derecho a la protección de datos personales y su reflejo en el consentimiento del interesado», *Revista de Derecho Político*, núm. 108, 2020, pp. 165-194 (disponible en https://revistas.uned.es/index.php/derechopolitico/article/download/27998/21775/63974; última consulta: 2 de junio de 2026).

[6]Warren, S. D. y Brandeis, L. D., «The Right to Privacy», *Harvard Law Review*, vol. IV, núm. 5, 1890, pp. 193-220 (disponible en https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html; última consulta: 2 de junio de 2026).

La progresiva expansión de las tecnologías digitales ha contribuido a replantear el alcance tradicional de la privacidad. En las sociedades contemporáneas, la protección de la persona ya no depende exclusivamente de la existencia de espacios físicos reservados, sino también de la capacidad de controlar la información que se genera de manera constante en la actividad cotidiana. La privacidad se proyecta así sobre ámbitos que trascienden la esfera íntima en sentido estricto y alcanza aquellas manifestaciones de la personalidad que permiten identificar, describir o perfilar a un individuo. Esta ampliación funcional explica que la protección jurídica de la privacidad haya evolucionado desde una concepción centrada en el secreto hacia otra basada en el control y la autonomía personal.[7]

La vinculación entre privacidad y autonomía individual resulta especialmente notable cuando se advierte que la posibilidad de controlar la información que circula sobre uno mismo es condición de la existencia de otras libertades fundamentales. Al que no lo tiene, se convierte en objeto de observación permanente, con las consecuencias inhibidoras que esto tiene para la libertad de expresión, la libre formación de la conciencia o el derecho de asociación. De esta manera, la privacidad no es un derecho aislado, sino una condición estructural del orden democrático y del Estado de Derecho.[8]

Esta dimensión filosófica ha encontrado expresión jurídica en distintas tradiciones constitucionales. En los ordenamientos de la Europa continental, la protección de la esfera privada del individuo se ha articulado históricamente en torno al concepto de dignidad de la persona, que en el caso español tiene su sede en el artículo 10.1 de la CE como fundamento del orden político y de la paz social. En el *common law* anglosajón, en cambio, la aproximación fue más pragmática y orientada a la tutela frente a injerencias concretas, lo que

[7]PIÑAR MAÑAS, J. L., «¿Existe privacidad?», en *Lecturas sobre privacidad y protección de datos*, Instituto Federal de Acceso a la Información y Protección de Datos, México, 2010.
[8]Saldaña, M. N., «"The Right to Privacy". La génesis de la protección de la privacidad en el sistema constitucional norteamericano: el centenario legado de Warren y Brandeis», *Revista de Derecho Político*, núm. 85, 2012, pp. 195-240 (disponible en https://revistas.uned.es/index.php/derechopolitico/article/download/10723/10242; última consulta: 2 de junio de 2026).

explica que la formulación canónica del derecho a la *privacy* surgiera precisamente en ese contexto[9]

Conviene subrayar que la privacidad, en su versión contemporánea, trasciende la mera protección de un espacio físico o de un conjunto de informaciones íntimas en sentido estricto. El fenómeno del tratamiento masivo de datos personales ha ensanchado extraordinariamente el campo de lo que merece protección jurídica. En la sociedad digital, incluso datos aparentemente irrelevantes tomados de forma aislada, como la localización geográfica en un momento dado, o el historial de búsquedas en internet, pueden, al ser combinados y sometidos a técnicas de análisis avanzadas, revelar aspectos profundos de la personalidad del individuo que este tiene todo el derecho a mantener reservados. En este escenario, la privacidad deviene un derecho de naturaleza informacional, íntimamente ligado a la protección de datos personales.[10]

La doctrina más reciente ha insistido, con razón, en que sin privacidad no hay democracia. Cuando el poder, sea político o económico, puede acceder de forma irrestricta a la información sobre los ciudadanos, se destruyen las condiciones que hacen posible la participación autónoma en la vida pública. El control masivo de datos puede utilizarse para manipular preferencias, diseñar estrategias de microtargeting electoral o simplemente disuadir conductas que, siendo completamente lícitas, el poder preferiría evitar. La defensa de la privacidad es, en este sentido, también defensa de la propia naturaleza abierta y plural del régimen democrático.[11]

1.2. Del *right to be let alone* a la autodeterminación informativa: evolución histórica

La historia del derecho a la privacidad como categoría jurídica comienza convencionalmente en 1890, con la publicación en la *Harvard Law Review* del célebre

[9] Martínez de Pisón, J., «El derecho a la intimidad: de la configuración inicial a los últimos desarrollos en la jurisprudencia constitucional», *Anuario de Filosofía del Derecho*, vol. XXXII, 2016, pp. 409-430 (disponible en https://dialnet.unirioja.es/descarga/articulo/5712518.pdf; última consulta: 2 de junio de 2026).

[10] Piñar Mañas, J. L., "El derecho a la protección de datos de carácter personal en la jurisprudencia del Tribunal de Justicia de las Comunidades Europeas", *Cuadernos de Derecho Público*, núms. 19-20, 2003, pp. 45 y ss. (disponible en https://revistasonline.inap.es/index.php/CDP/article/download/692/747/925; última consulta 2/06/2026).

[11] Casas Baamonde, M. E. (coord.), *op. cit.*, pp. 11-12

artículo de Samuel D. Warren y Louis D. Brandeis titulado "The Right to Privacy". Sus autores respondían al contexto de su tiempo: el desarrollo tecnológico de la fotografía instantánea y de una prensa sensacionalista que comenzaba a invadir la esfera íntima de las personas, publicando retratos y detalles de su vida privada sin su consentimiento. Warren y Brandeis formularon entonces la idea de que el common law debía reconocer un derecho a ser dejado en paz "*the right to be let alone*", entendido como la protección de la inviolabilidad de la personalidad frente a toda injerencia no consentida.[12] El impacto de ese texto en la cultura jurídica angloamericana fue enorme y duradero. Su influencia puede rastrearse en numerosas sentencias del Tribunal Supremo de los Estados Unidos, y su huella conceptual se proyecta hasta los debates contemporáneos sobre la privacidad en la era digital. Sin embargo, la formulación original de Warren y Brandeis respondía todavía a una concepción principalmente defensiva del derecho, esta buscaba proteger al individuo frente a intromisiones externas, pero no le reconocía aún un poder positivo de control sobre su propia información. El paso de esa visión defensiva a una concepción activa y dinámica de la privacidad fue el resultado de la evolución jurídica e institucional producida durante la segunda mitad del siglo XX.[13]

Esa evolución estuvo impulsada, en gran medida, por el desarrollo de las tecnologías de la información. Fue en las décadas de los sesenta y setenta del pasado siglo cuando comenzó a hacerse evidente que el tratamiento automatizado de datos personales planteaba riesgos cualitativamente distintos de los que habían preocupado anteriormente. Ya no se trataba sólo de que, por ejemplo, un periódico publicara una fotografía indiscreta. Las nuevas posibilidades de almacenamiento, cruce y análisis de información permitían elaborar perfiles detallados de las personas que podían ser utilizados de formas muy diversas, tanto por el Estado como por los operadores privados. Esta nueva realidad dio lugar, desde los años

[12] Warren, S. D. y Brandeis, L. D., *op. cit.* Los autores invocaban la formulación de Thomas Cooley: «the right to be let alone», recogida en *A Treatise on the Law of Torts* (2.ª ed., Chicago, 1888, p. 29).
[13] Saldaña, M. N., *op. cit.*, pp. 197-200. La autora señala que el artículo de Warren y Brandeis ha sido uno de los más citados por la doctrina y jurisprudencia norteamericana, representando el ensayo fundacional de la protección de la esfera privada en los Estados Unidos.

setenta, a un movimiento legislativo en toda Europa que produjo las primeras leyes específicas de protección de datos.[14]

La respuesta jurídico-dogmática más elaborada a este nuevo escenario fue la teoría de la autodeterminación informativa, desarrollada en la sentencia del Tribunal Constitucional Federal alemán de 15 de diciembre de 1983, conocida como la Sentencia del Censo[15]. Ese pronunciamiento reconoció que todo individuo tiene el derecho fundamental a decidir básicamente por sí mismo cuándo y dentro de qué límites procede revelar situaciones referentes a su propia vida, reformulando así el derecho a la privacidad como un poder activo de control sobre la información personal. Esta concepción, que trasciende la mera protección pasiva frente a las intromisiones y es la que ha inspirado el modelo europeo de protección de datos y se encuentra hoy incorporada al artículo 8 de la Carta de Derechos Fundamentales de la Unión Europea.[16]

La transformación digital no ha supuesto únicamente la aparición de nuevos instrumentos técnicos, sino una modificación profunda del modo en que se ejercen y se protegen los derechos. El Derecho se enfrenta ahora a relaciones sociales mediadas por plataformas, algoritmos y sistemas de tratamiento masivo de información, lo que obliga a reinterpretar categorías jurídicas clásicas a la luz de una realidad tecnológica cambiante. Desde esta perspectiva, la privacidad deja de ser un derecho concebido sólo frente a intromisiones puntuales y pasa a operar como una garantía transversal frente a formas continuas, invisibles y acumulativas de tratamiento de datos personales.[17]

---

[14] Piñar Mañas, J. L., «El derecho a la protección de datos de carácter personal…», *op. cit.*, pp. 46-48. El autor recuerda que desde los años sesenta del siglo XX comenzó a generalizarse el uso de nuevas tecnologías que no solo permitían obtener y almacenar grandes volúmenes de datos, sino someterlos a tratamiento, incrementando de forma espectacular las posibilidades de injerencia en la intimidad.

[15] Sentencia del Tribunal Constitucional Federal alemán (Bundesverfassungsgericht), Sala Primera, de 15 de diciembre de 1983, asunto 1 BvR 209/83 y acumulados (Sentencia del Censo, Volkszählungsurteil), BVerfGE 65, 1. El Tribunal acuñó en ella el derecho a la autodeterminación informativa (informationelle Selbstbestimmung).

[16]Polo Roca, A., *op. cit.*, p. 168. El autor señala que el derecho a la autodeterminación informativa goza de reconocimiento y garantía en dos de las normas de constitución material de la UE: el TFUE y la CDFUE.

[17]DE LA QUADRA-SALCEDO FERNÁNDEZ DEL CASTILLO, T. y PIÑAR MAÑAS, J. L. (dirs.), *Sociedad digital y Derecho*, BARRIO ANDRÉS, M. y TORREGROSA VÁZQUEZ, J. (coords.), Boletín Oficial del Estado, Ministerio de Industria, Comercio y Turismo y Red.es, Madrid, 2018.

La evolución descrita no fue lineal ni estuvo exenta de tensiones doctrinales, políticas y jurídicas. En la tradición angloamericana, la privacidad continuó siendo concebida durante largo tiempo desde una perspectiva más vinculada a la protección de la esfera individual frente a injerencias externas, estrechamente relacionada con la propiedad privada, la libertad contractual y la autonomía de la voluntad. Esta concepción, de carácter más liberal e individualista, explica en gran medida las diferencias sustanciales que todavía hoy existen entre el modelo estadounidense y el modelo europeo de protección de datos personales. Mientras que en Estados Unidos la protección de la información personal ha evolucionado tradicionalmente a través de regulaciones sectoriales y de mecanismos de autorregulación, en Europa se ha desarrollado una visión más amplia y garantista de la tutela de la persona frente a los riesgos derivados del tratamiento de datos. En el contexto europeo, la estrecha vinculación entre privacidad, dignidad humana y libre desarrollo de la personalidad proporcionó el fundamento teórico necesario para construir un sistema de protección más sólido y uniforme. Esta evolución permitió superar una concepción meramente defensiva de la privacidad para configurarla como un verdadero derecho de control sobre la información personal. Como resultado de este proceso, la protección de datos dejó de entenderse únicamente como una manifestación del derecho a la intimidad y adquirió autonomía propia dentro del catálogo de derechos fundamentales. La culminación de esta evolución se produjo con el reconocimiento expreso de la protección de datos personales como derecho fundamental autónomo en el ámbito del Derecho de la Unión Europea, consolidando así un modelo jurídico que sitúa a la persona y a la protección de su información en el centro del sistema de garantías frente a los desafíos derivados de la sociedad digital.[18]

1.3. Reconocimiento constitucional y en la Carta de Derechos Fundamentales de la UE

El reconocimiento constitucional del derecho a la privacidad en el ordenamiento español se articula fundamentalmente a través del artículo 18 de la CE. En su apartado primero, ese precepto garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen. En su apartado cuarto, establece que la ley limitará el uso de la informática

[18]Martínez de Pisón, J., *op. cit.*, pp. 411-412. El autor subraya que Warren y Brandeis, cuando esbozaron su definición en 1890, no podían imaginar la incidencia de la informática en la vida privada de las personas

para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos. Esta última disposición, cuya relevancia fue subrayada por el Tribunal Constitucional en su sentencia 292/2000, de 30 de noviembre[19], constituye el fundamento constitucional específico del derecho a la protección de datos personales en España.[20]

La doctrina constitucional española ha elaborado, a partir de esa base normativa, una distinción conceptualmente relevante entre el derecho a la intimidad del artículo 18.1 CE y el derecho a la protección de datos del artículo 18.4 CE. El primero protege una esfera reservada de la vida personal y familiar frente a intromisiones externas; el segundo, en cambio, garantiza a su titular un poder de control sobre la información que le concierne, con independencia de que esa información pertenezca o no al ámbito íntimo en sentido estricto. Así, la protección de datos es materialmente más amplia que la intimidad, pues puede referirse a datos que, considerados aisladamente, no serían íntimos pero que, tratados en su conjunto, permiten elaborar un perfil de la persona que afecta a su dignidad y a su libertad.[21]

En el ámbito del Derecho de la Unión Europea, la Carta de los Derechos Fundamentales proclamada en Niza en el año 2000 y dotada de efecto vinculante con el Tratado de Lisboa en 2009 distingue, en sus artículos 7 y 8, entre el derecho al respeto de la vida privada y familiar y el derecho a la protección de datos personales. El artículo 8 de la Carta establece que toda persona tiene derecho a la protección de sus datos de carácter personal, que 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, y que toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a

---

[19] Sentencia del Tribunal Constitucional (Pleno) núm. 292/2000, de 30 de noviembre, FF.JJ. 6 y 7 (recurso de inconstitucionalidad núm. 1463/2000, promovido por el Defensor del Pueblo contra la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal), BOE núm. 4, de 4 de enero de 2001.

[20] Constitución Española, arts. 18.1 y 18.4.

[21] Polo Roca, A., *op. cit.*, pp. 167-168. El autor señala que el derecho fundamental a la protección de datos se encuentra reconocido en el art. 18.4 CE, el art. 8 CDFUE y el art. 16 TFUE.

obtener su rectificación. El apartado tercero añade que el respeto de estas normas quedará sujeto al control de una autoridad independiente.[22]

La distinción entre el artículo 7 y el artículo 8 de la Carta no es meramente formal. El artículo 7 conecta con la tradición del Convenio Europeo de Derechos Humanos (CEDH) y su artículo 8, que tutela la vida privada y familiar en sentido amplio; el artículo 8 de la Carta, en cambio, constituye un derecho fundamental autónomo específicamente orientado a la protección de datos personales, con un contenido normativo propio que incluye los principios de finalidad, calidad y consentimiento, así como el derecho de acceso y rectificación y el sometimiento al control de una autoridad independiente. Esta autonomía del derecho a la protección de datos respecto del derecho a la vida privada es uno de los rasgos más característicos del modelo europeo y uno de los aspectos en los que este se diferencia más claramente de otros sistemas jurídicos.[23]

El Tribunal Constitucional español, por su parte, ha elaborado a lo largo de varias décadas una jurisprudencia matizada sobre el contenido y los límites del derecho a la intimidad y del derecho a la protección de datos. En particular, la STC 292/2000 como se menciona anteriormente es la referencia ineludible en esta materia: en ella, el Tribunal afirmó que la protección de datos personales tiene por objeto garantizar a las personas un poder de control sobre sus datos, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado, y que ese poder de disposición y control entraña que la persona a quien esos datos le afecten debe ser el árbitro de la información que sobre ella se revela o comunica.[24]

---

[22] Carta de los Derechos Fundamentales de la Unión Europea, arts. 7 y 8, DOUE C 326, de 26 de octubre de 2012 (disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:12012P/TXT; última consulta: 2 de junio de 2026).

[23] Piñar Mañas, J. L., «Derecho e innovación. Privacidad y otros derechos en la sociedad digital», en Casas Baamonde, M. E. (coord.), *El derecho a la protección de datos personales en la sociedad digital*, Fundación Ramón Areces, Madrid, 2020, pp. 39-63 (disponible en https://www.fundacionareces.es/recursos/doc/portal/2018/03/20/el-derecho-a-la-proteccion-de-datos-personales.pdf; última consulta: 2 de junio de 2026).

[24] Martínez de Pisón, J., *op. cit.*, pp. 415-416. El autor señala que el Tribunal Constitucional ha elaborado una doctrina consolidada sobre el derecho a la intimidad a partir del art. 18.1 CE, distinguiéndolo del derecho a la protección de datos del art. 18.4 CE.

1.4. Jurisprudencia clave: TEDH y TJUE

El Tribunal Europeo de Derechos Humanos ha desempeñado un papel fundamental en la configuración jurídica del derecho a la vida privada en el ámbito europeo a través de la interpretación del artículo 8 del Convenio Europeo de Derechos Humanos. Entre los pronunciamientos más relevantes destaca la sentencia de Gran Sala del caso Von Hannover c. Alemania (n.º 2), de 7 de febrero de 2012, en la que el Tribunal estableció los criterios para ponderar el derecho a la vida privada de las personas públicas con la libertad de expresión e información.El TEDH afirmó que el hecho de que una persona sea conocida no convierte automáticamente en legítima cualquier publicación de datos o imágenes referidos a ella, y que el juicio de proporcionalidad exige atender a si la información contribuye a un debate de interés general, a la notoriedad de la persona afectada, al objeto de la noticia, al comportamiento anterior del afectado y al contenido, forma y consecuencias de la publicación.[25]

En el ámbito del Derecho de la Unión Europea, la sentencia del TJUE de 13 de mayo de 2014 en el asunto Google Spain (C-131/12) ha sido uno de los pronunciamientos más influyentes de los últimos años en materia de protección de datos. En ese asunto, planteado a instancia de la Audiencia Nacional española, el Tribunal tuvo que pronunciarse sobre si el gestor de un motor de búsqueda en internet es responsable del tratamiento de los datos personales que aparecen en las páginas web publicadas por terceros y que dicho motor indexa, almacena y pone a disposición del público. La respuesta del Tribunal fue afirmativa.[26]

---

[25]Sentencia del Tribunal Europeo de Derechos Humanos (Gran Sala), asunto *Von Hannover c. Alemania (n.º 2)*, de 7 de febrero de 2012, demandas núms. 40660/08 y 60641/08 (disponible en https://globalfreedomofexpression.columbia.edu/cases/von-hannover-v-germany-no-2/?lang=es; última consulta: 2 de junio de 2026).

[26] Sentencia del Tribunal de Justicia de la Unión Europea de 13 de mayo de 2014, asunto C-131/12, *Google Spain SL y Google Inc. c. Agencia Española de Protección de Datos (AEPD) y Mario Costeja González* (disponible en https://www.abogacia.es/wp-content/uploads/2014/05/Sentencia-131-12-TJUE-derecho-al-olvido.pdf; última consulta: 2 de junio de 2026).

La sentencia Google Spain es especialmente relevante por dos razones. En primer lugar, afirmó con claridad que la actividad de un motor de búsqueda constituye un tratamiento de datos personales en el sentido de la Directiva 95/46/CE y que el operador de dicho motor debe ser considerado responsable de ese tratamiento. En segundo lugar, y de manera particularmente significativa, el Tribunal reconoció el denominado derecho al olvido: el interesado puede exigir al gestor del motor de búsqueda que retire de su lista de resultados vínculos a páginas web que contengan información sobre él, aunque esa información hubiera sido publicada lícitamente por los editores de esas páginas. Este reconocimiento supuso una extensión notable de los derechos del interesado que la normativa positiva no preveía de forma explícita y que el RGPD recogería posteriormente en su artículo 17 como derecho de supresión.[27]

La jurisprudencia del TJUE en materia de protección de datos no se limita, sin embargo, a ese pronunciamiento. Desde los primeros casos de los años sesenta y setenta, el Tribunal fue reconociendo gradualmente que los derechos fundamentales, incluido el derecho al respeto de la vida privada, forman parte de los principios generales del ordenamiento comunitario cuyo respeto garantiza el propio Tribunal. Esta construcción jurisprudencial, que corrió en paralelo a la elaboración legislativa de las primeras directivas de protección de datos, sentó las bases de lo que hoy constituye el sistema europeo de protección de datos personales, caracterizado por un nivel de garantías que no tiene similitud en el derecho comparado.[28]

La importancia del sistema europeo reside precisamente en que no ofrece una protección aislada o fragmentaria, sino un marco común en el que confluyen el Convenio Europeo de

---

[27] Sentencia del Tribunal de Justicia de la Unión Europea de 13 de mayo de 2014, asunto C-131/12, *Google Spain*, apartados 38 y 87-88. El Tribunal señaló que el gestor de un motor de búsqueda es responsable del tratamiento que efectúa de los datos personales que aparecen en páginas web publicadas por terceros, y que el interesado puede solicitar que la información de que se trata ya no se ponga a disposición del público en general mediante su inclusión en la lista de resultados.

[28] Piñar Mañas, J. L., «El derecho a la protección de datos de carácter personal…», *op. cit.*, pp. 48-56. El autor analiza detalladamente la evolución de la jurisprudencia del TJUE en materia de protección de datos desde el caso *Stauder* de 1969 hasta las primeras grandes resoluciones sobre la Directiva 95/46/CE.

Derechos Humanos, la Carta de Derechos Fundamentales de la Unión Europea y la jurisprudencia del TEDH y del TJUE. Esta convergencia ha permitido construir un estándar europeo especialmente exigente, en el que la privacidad y la protección de datos se entienden como garantías indispensables para preservar la dignidad, la autonomía y el libre desarrollo de la persona en contextos tecnológicos cada vez más complejos.[29]

La importancia atribuida por el Derecho de la Unión a la protección de los datos personales quedó especialmente reflejada en la sentencia Digital Rights Ireland. En esta resolución, el Tribunal de Justicia subrayó que las medidas de conservación generalizada de información relativa a las comunicaciones electrónicas pueden afectar de forma intensa a la vida privada de los ciudadanos cuando permiten conocer aspectos relevantes de sus hábitos, relaciones o actividades. La decisión constituye un ejemplo significativo de cómo la protección de datos ha dejado de ser una cuestión meramente administrativa para convertirse en un elemento esencial en la defensa de los derechos fundamentales dentro del entorno digital.[30]

La consolidación de un auténtico modelo europeo de protección de datos constituye uno de los desarrollos más relevantes del constitucionalismo contemporáneo. A diferencia de otros ordenamientos jurídicos, en los que la privacidad continúa vinculada principalmente a la protección frente a intromisiones externas, el sistema europeo ha evolucionado hacia una concepción más amplia basada en el control de la información personal y en la garantía de la autonomía individual.

Esta evolución ha sido posible gracias a la interacción entre diferentes instrumentos normativos y jurisdiccionales. Por un lado, el Convenio Europeo de Derechos Humanos ha permitido construir una protección progresiva de la vida privada a través de la jurisprudencia del Tribunal Europeo de Derechos Humanos. Por otro, la Unión Europea ha desarrollado un

---

[29] AGENCIA DE LOS DERECHOS FUNDAMENTALES DE LA UNIÓN EUROPEA y CONSEJO DE EUROPA, *Manual de legislación europea en materia de protección de datos*, Oficina de Publicaciones de la Unión Europea, Luxemburgo, 2018.

[30] STJUE de 8 de abril de 2014, asuntos acumulados C-293/12 y C-594/12, *Digital Rights Ireland Ltd*.

marco jurídico específico en materia de protección de datos que culmina con el reconocimiento de este derecho como una garantía autónoma en el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea.

La coexistencia de ambos sistemas no ha generado una duplicidad de protección, sino un fenómeno de refuerzo mutuo. Las resoluciones del TEDH y del TJUE han contribuido a perfilar estándares comunes sobre principios como la proporcionalidad, la necesidad de las restricciones, la transparencia en el tratamiento de información personal o la existencia de mecanismos efectivos de tutela para los ciudadanos. De este modo, la protección de datos se ha configurado como un elemento esencial para el funcionamiento de las sociedades democráticas avanzadas.

La relevancia de este modelo europeo resulta especialmente visible en el contexto de la transformación digital. El desarrollo de internet, las plataformas digitales, la computación en la nube y los sistemas de inteligencia artificial ha incrementado exponencialmente la capacidad de recopilar, almacenar y procesar información relativa a las personas. Ante esta realidad, la protección de datos ya no puede entenderse únicamente como una cuestión técnica o administrativa, sino como una condición necesaria para el ejercicio efectivo de otros derechos fundamentales, entre ellos la libertad de expresión, la libertad ideológica, la libertad de asociación o el derecho a la participación política.

Desde esta perspectiva, la protección de datos actúa como una garantía transversal que contribuye a preservar espacios de autonomía personal frente a dinámicas de vigilancia, monitorización o perfilado excesivo. El reconocimiento de facultades como el acceso, la rectificación, la supresión o la limitación del tratamiento responde precisamente a la necesidad de mantener un equilibrio adecuado entre las posibilidades que ofrece la innovación tecnológica y la protección de la dignidad humana. En consecuencia, el modelo europeo no persigue obstaculizar el desarrollo tecnológico, sino asegurar que dicho desarrollo

se produzca dentro de un marco respetuoso con los derechos fundamentales y con los valores propios de una sociedad democrática.[31]

Capítulo 2. El marco normativo de protección de datos

2.1. El RGPD: principios, derechos y obligaciones

El Reglamento (UE) 2016/679, conocido universalmente como RGPD, entró en aplicación el 25 de mayo de 2018 y supuso la reforma más ambiciosa del marco europeo de protección de datos desde la Directiva 95/46/CE. A diferencia de su predecesora, el RGPD es directamente aplicable en todos los Estados miembros sin necesidad de transposición aunque sí requiere, en determinadas materias, de leyes nacionales de desarrollo modificaciones, lo que ha contribuido a una mayor uniformidad en la aplicación de las normas de protección de datos en todo el territorio de la Unión Europea.[32]

El núcleo del RGPD está constituido por un conjunto de principios que deben presidir todo tratamiento de datos personales y que se enuncian en su artículo 5. Esos principios son: la licitud, lealtad y transparencia, que exige que el tratamiento tenga una base jurídica y que el interesado reciba información clara sobre él; la limitación de la finalidad, que impide tratar los datos para fines distintos de los que justificaron su recogida; la minimización de datos, que obliga a tratar solo los datos estrictamente necesarios para la finalidad perseguida; la exactitud, que impone el deber de mantener los datos actualizados; la limitación del plazo de conservación, que prohíbe guardar los datos más tiempo del necesario; y la integridad y confidencialidad, que obliga al responsable del tratamiento a adoptar las medidas técnicas y organizativas adecuadas para garantizar la seguridad de los datos.[33]

---

[31] AGENCIA DE LOS DERECHOS FUNDAMENTALES DE LA UNIÓN EUROPEA y CONSEJO DE EUROPA, *Manual de legislación europea en materia de protección de datos.*

[32] Reglamento (UE) 2016/679, arts. 5, 6, 7 y 12-22.

[33] Polo Roca, A., *op. cit.*, pp. 168-175. El autor analiza en detalle el sistema de principios del RGPD y su relación con el consentimiento del interesado.

El catálogo de derechos del interesado que reconoce el RGPD es notablemente amplio y constituye una de las principales novedades respecto del régimen anterior. Incluye el derecho de acceso, de rectificación, de supresión; que recoge y amplía el derecho al olvido perfilado por la jurisprudencia, de limitación del tratamiento, de portabilidad de los datos, de oposición y de no ser objeto de decisiones automatizadas individualizadas, incluida la elaboración de perfiles. El ejercicio de estos derechos debe ser gratuito para el interesado, y el responsable del tratamiento está obligado a responder a las solicitudes en el plazo de un mes, prorrogable en casos de especial complejidad.

Junto a los derechos del interesado, el RGPD introduce un conjunto de obligaciones para los responsables y encargados del tratamiento que van mucho más allá de lo que preveía la normativa anterior. Entre ellas destaca el principio de responsabilidad proactiva o *accountability*, que obliga al responsable no solo a cumplir con las normas de protección de datos sino también a poder demostrar ese cumplimiento. Esta exigencia se traduce en la necesidad de mantener registros de actividades de tratamiento, realizar evaluaciones de impacto en determinados supuestos de alto riesgo, adoptar medidas de seguridad apropiadas, y designar un delegado de protección de datos cuando concurran determinadas circunstancias.[34]

El sistema de sanciones previsto en el RGPD es, asimismo, significativamente más riguroso que el de la normativa derogada. El artículo 83 establece multas de hasta veinte millones de euros o, en el caso de una empresa, del cuatro por ciento del volumen de negocio total anual global del ejercicio financiero anterior si esta cifra fuera superior, para las infracciones más graves. Esta escala sancionadora ha demostrado tener un efecto disuasorio real, como lo prueba la serie de grandes multas impuestas por distintas autoridades de control europeas en los años transcurridos desde la aplicación del Reglamento.

[34]Piñar Mañas, J. L., «Derecho e innovación…», *op. cit.*, pp. 58-62. El autor subraya que el RGPD introduce el principio de responsabilidad proactiva (accountability), que obliga al responsable del tratamiento a demostrar el cumplimiento de los principios de protección de datos.

2.2. La LOPDGDD: adaptación española

La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD) constituye el principal instrumento de adaptación del ordenamiento jurídico español al RGPD. Su aprobación supuso la derogación de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal (LOPD), que había sido durante casi veinte años el eje vertebrador de la protección de datos en España. La LOPDGDD complementa el RGPD en los espacios de regulación que el Reglamento expresamente defiere a los legisladores nacionales, como el tratamiento de datos en el ámbito laboral, el tratamiento con fines de archivo en interés público, o el régimen de los menores en las redes sociales y añade, además, una regulación pionera de los denominados derechos digitales.[35]

Entre las materias específicamente reguladas por la LOPDGDD más allá de lo exigido por el RGPD, destaca el Título X de la ley, dedicado a los denominados derechos digitales. Este título reconoce, entre otros, el derecho a la neutralidad en internet, el derecho al acceso universal a internet, el derecho a la seguridad digital, el derecho a la educación digital, el derecho de rectificación en internet, el derecho a la actualización de informaciones en medios de comunicación digitales, el derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral, el derecho a la desconexión digital y el derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo. Esta regulación sitúa a España en el primero de los ordenamientos que han abordado de forma expresa las nuevas formas de afectación de los derechos fundamentales en el entorno digital[36]

En lo que respecta a la relación entre protección de datos y acceso a la información pública, la LOPDGDD establece un marco de ponderación que resulta de particular relevancia en el ámbito de la transparencia y la administración pública. La doctrina ha

[35]Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, BOE núm. 294, de 6 de diciembre de 2018 (disponible en https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673; última consulta: 2 de junio de 2026).

[36] Piñar Mañas, J. L., «Derecho e innovación…», *op. cit.*, pp. 61-63. El autor destaca que la LOPDGDD, al incluir una regulación específica de los derechos digitales, va más allá de lo exigido por el RGPD y responde a la cláusula del art. 18.4 CE.

señalado que la protección de datos personales actúa como límite al derecho de acceso a la información pública reconocido en la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, de manera que cuando la solicitud de acceso se refiera a datos de carácter personal de terceros, las autoridades están obligadas a realizar un juicio de proporcionalidad entre el interés público en la transparencia y el derecho del titular de los datos a controlar la información que le concierne[37]

La LOPDGDD también regula el estatuto del Delegado de Protección de Datos (en adelante, DPD), configurado en el RGPD como una pieza clave del sistema de cumplimiento. En el contexto español, la ley extiende la obligación de designar DPD a determinadas categorías de entidades públicas y privadas, y establece que su designación debe recaer en una persona con conocimientos especializados en la normativa de protección de datos. El DPD actúa como interlocutor entre el responsable del tratamiento y la Agencia Española de Protección de Datos, y tiene encomendadas funciones de asesoramiento, supervisión y cooperación con la autoridad de control.

2.3. Autoridades de control: AEPD y Comité Europeo de Protección de Datos

El RGPD articula un sistema de supervisión basado en la existencia de autoridades de control independientes en cada Estado miembro, cuya actuación se coordina a nivel europeo a través del Comité Europeo de Protección de Datos (en adelante, CEPD). En España, la Agencia Española de Protección de Datos (en adelante, AEPD), creada originariamente por la LOPD de 1999, actúa como autoridad de control competente para el sector privado y para el sector público, con la excepción de los organismos de las comunidades autónomas que cuenten con su propia autoridad de control autonómica.[38]

---

[37]Hernández López, J. M., «Protección de datos, intimidad y acceso a la información pública. Ponderación y proporcionalidad», *Revista Canaria de Administración Pública*, núm. 5, 2025, pp. 79-105 (disponible en https://revistacanarias.tirant.com/index.php/revista-canaria/article/download/79/70/187; última consulta: 2 de junio de 2026).

[38]Comité Europeo de Protección de Datos, *Marco legal del CEPD* (disponible en https://www.edpb.europa.eu/about-edpb/about-edpb/legal-framework_es; última consulta: 2 de junio de 2026).

La AEPD tiene encomendadas funciones de muy diversa índole: la supervisión del cumplimiento de la normativa de protección de datos, la resolución de reclamaciones de los ciudadanos, la imposición de sanciones, la emisión de directrices e informes, y la cooperación con el CEPD y con las autoridades de control de otros Estados miembros. En los últimos años, la Agencia ha intensificado su actividad normativa y orientadora, publicando guías prácticas de gran utilidad para responsables y encargados de tratamiento, entre las que destaca la Guía para la notificación de brechas de datos personales, cuyo contenido constituye una referencia ineludible para la gestión de incidentes de seguridad con afectación a datos personales.[39]

El Comité Europeo de Protección de Datos, por su parte, es el organismo de la Unión Europea integrado por los representantes de las autoridades de control de los distintos Estados miembros y por el Supervisor Europeo de Protección de Datos. Su función principal es garantizar la aplicación coherente del RGPD en todo el Espacio Económico Europeo, lo que implica la adopción de directrices, recomendaciones y buenas prácticas, así como la resolución de los conflictos que puedan surgir entre las autoridades de control nacionales en los procedimientos transfronterizos. Las directrices del CEPD tienen un valor interpretativo de primer orden, y su seguimiento por parte de los operadores jurídicos es esencial para garantizar el cumplimiento del RGPD en sus ámbitos más controvertidos.

PARTE II: LA CIBERSEGURIDAD COMO GARANTÍA JURÍDICA

Capítulo 3. Privacidad y ciberseguridad como una relación necesaria

3.1. Ciberseguridad como obligación jurídica, no solo técnica

Una de las contribuciones más relevantes del RGPD al desarrollo del derecho de la protección de datos ha sido la de elevar la ciberseguridad de categoría puramente técnica a

[39] Agencia Española de Protección de Datos, *Guía para la notificación de brechas de datos personales* (versión de junio de 2021), p. 2 (disponible en https://www.aepd.es/guias/guia-brechas-seguridad.pdf; última consulta: 2 de junio de 2026).

categoría jurídica de primer orden. El artículo 32 del Reglamento establece la obligación de adoptar medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como los riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas.[40] Esta caracterización de la seguridad como obligación jurídica tiene consecuencias de gran relevancia práctica. En primer lugar, implica que el incumplimiento de las obligaciones de seguridad puede dar lugar a sanciones administrativas de considerable cuantía, con independencia de que ese incumplimiento haya provocado efectivamente una brecha de seguridad. En segundo lugar, la exigencia de medidas "apropiadas" al riesgo supone que no existe un estándar único de seguridad válido para todos los tratamientos: el responsable está obligado a realizar un análisis de riesgos que le permita determinar qué medidas son adecuadas en función de las características concretas de su actividad. En tercer lugar, el carácter dinámico de la obligación que debe adaptarse al estado de la técnica y a la evolución del panorama de amenazas, que exige una revisión y actualización periódica de las medidas adoptadas. [41]

La Directiva NIS2, adoptada en diciembre de 2022 y que sustituyó a la Directiva NIS de 2016, ha reforzado y ampliado el marco europeo de ciberseguridad. Su ámbito de aplicación se extiende a un número mayor de sectores y entidades que la directiva precedente, y establece requisitos mínimos de ciberseguridad más exigentes para las entidades esenciales e importantes, que incluyen la obligación de adoptar medidas de gestión de riesgos, de notificar los incidentes significativos a las autoridades competentes en plazos muy estrictos, y de garantizar la seguridad de la cadena de suministro. La NIS2 ha de entenderse en articulación con el RGPD: aunque son instrumentos normativos distintos, responden a objetivos complementarios y, en muchos casos, las medidas de seguridad exigidas por la

[40] Reglamento (UE) 2016/679, art. 32. El precepto exige la adopción de medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, incluyendo, según proceda, la seudonimización y el cifrado de datos, la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento, y la capacidad de restaurar la disponibilidad y el acceso a los datos en caso de incidente físico o técnico.
[41] Agencia Española de Protección de Datos, *Guía para la notificación de brechas…*, *op. cit.*, pp. 5-8.

NIS2 son también las medidas que el RGPD exige para la protección de los datos personales.[42]

La relación entre ciberseguridad y protección de datos no es, en todo caso, de simple subordinación de la primera a la segunda. La ciberseguridad tiene una dimensión propia que trasciende la protección de datos personales: incluye la protección de infraestructuras críticas, de sistemas de control industrial, de redes de comunicaciones y de una multiplicidad de activos digitales que pueden no contener datos personales pero cuya integridad y disponibilidad son esenciales para el funcionamiento de la sociedad y la economía. Lo que sí es cierto es que, en aquellos supuestos en los que los sistemas comprometidos contienen datos personales, la ciberseguridad deviene una exigencia jurídica directa derivada del ordenamiento de protección de datos.

3.2. *Privacy by design y privacy by default* (art. 25 RGPD)

El artículo 25 del RGPD introduce dos principios de notable relevancia práctica que representan un cambio de paradigma respecto de la aproximación tradicional a la protección de datos: la protección de datos desde el diseño (*privacy by design*) y la protección de datos por defecto (*privacy by default*). Ambos principios responden a la misma idea fundamental: la protección de datos no debe abordarse como un añadido externo que se incorpora a los sistemas y procesos una vez que estos han sido diseñados, sino como una dimensión intrínseca que debe estar presente desde el momento mismo en que se concibe el tratamiento.[43]

La privacy by design implica que el responsable del tratamiento, teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del

[42] Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión (Directiva NIS2), DOUE L 333, de 27 de diciembre de 2022 (disponible en https://www.boe.es/buscar/doc.php?id=DOUE-L-2022-81963; última consulta: 2 de junio de 2026).

[43] Agencia Española de Protección de Datos, *Guía de Privacidad desde el Diseño* (versión de octubre de 2019), pp. 5-7 (disponible en https://www.aepd.es/guias/guia-privacidad-desde-diseno.pdf; última consulta: 2 de junio de 2026). El concepto fue desarrollado por la Comisionada de Protección de Datos de Ontario, Ann Cavoukian, en la década de los noventa, y fue aceptado internacionalmente en la 32.ª Conferencia Internacional de Comisionados de Protección de Datos y Privacidad (Jerusalén, 2010).

tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, aplicará desde el momento de la determinación de los medios de tratamiento y en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos. [44]

Lo que se conoce como *privacy by default*, por su parte, exige que el responsable aplique las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplica a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. En particular, tales medidas garantizarán que, por defecto, los datos personales no sean accesibles, sin la intervención del interesado, a un número indeterminado de personas físicas. La guía de privacidad desde el diseño de la AEPD ha desarrollado en detalle los siete principios fundacionales de este enfoque, que van desde la actitud proactiva y preventiva hasta el respeto por la privacidad del usuario como valor central de toda la estructura del sistema.[45]

3.3. Brechas de seguridad: notificación, consecuencias y gestión

El RGPD introduce por primera vez en el ordenamiento europeo una obligación general de notificación de las brechas de seguridad de datos personales. Antes de su entrada en vigor, solo existían obligaciones de notificación en sectores específicos

[44] Reglamento (UE) 2016/679, art. 25. El precepto distingue entre la protección de datos desde el diseño —que obliga a aplicar medidas técnicas y organizativas apropiadas desde la fase de determinación de los medios de tratamiento— y la protección de datos por defecto —que exige que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento—.

[45] Agencia Española de Protección de Datos, *Guía de Privacidad desde el Diseño…*, *op. cit.*, pp. 7-10. La guía describe los siete principios fundacionales de la privacidad desde el diseño: carácter proactivo; privacidad como configuración predeterminada; privacidad incorporada en el diseño; funcionalidad total; seguridad en todo el ciclo de vida; visibilidad y transparencia; y respeto por la privacidad del usuario.

fundamentalmente, el de las telecomunicaciones. El Reglamento extiende esta obligación a todos los responsables del tratamiento y establece un régimen de doble notificación: por un lado, a la autoridad de control competente; por otro, a los propios interesados afectados cuando la brecha pueda suponer un alto riesgo para sus derechos y libertades.[46]

El plazo para notificar a la autoridad de control es de setenta y dos horas desde que el responsable haya tenido constancia de la brecha, salvo que sea improbable que la violación de la seguridad constituya un riesgo para los derechos y libertades de las personas físicas. Cuando la notificación no pueda realizarse en ese plazo, deberá ir acompañada de una indicación de los motivos del retraso. La notificación debe contener, al menos, una descripción de la naturaleza de la violación, las categorías y el número aproximado de interesados y de registros afectados, los datos de contacto del DPD, las posibles consecuencias de la violación y las medidas adoptadas o propuestas para remediar la situación. [47]

La gestión de una brecha de seguridad no se agota en la obligación de notificación. La AEPD ha elaborado una guía detallada que describe el proceso completo de gestión de incidentes, desde la detección y contención inicial hasta las medidas de recuperación y la evaluación posterior. Este proceso incluye la evaluación del riesgo para los derechos y libertades de los afectados, que determinará si procede la notificación a la autoridad de control y la comunicación a los interesados, y la adopción de medidas correctoras que eviten que el incidente se repita o que reduzcan sus consecuencias. La documentación de todo el proceso es esencial, tanto para demostrar el cumplimiento de las obligaciones de notificación como para satisfacer el principio de responsabilidad proactiva.

---

[46] Agencia Española de Protección de Datos, *Guía para la notificación de brechas…*, *op. cit.*, pp. 8-14.

[47] Reglamento (UE) 2016/679, arts. 33 y 34. El art. 33.1 establece la obligación de notificar a la autoridad de control competente sin dilación indebida y, de ser posible, a más tardar 72 horas después de que el responsable haya tenido constancia de la brecha. El art. 34.1 obliga a comunicar la brecha al interesado cuando sea probable que entrañe un alto riesgo para sus derechos y libertades.

3.4. El Esquema Nacional de Seguridad y la Directiva NIS2

El Esquema Nacional de Seguridad (en adelante, ENS), regulado actualmente por el Real Decreto 311/2022, de 3 de mayo, establece el marco de referencia en materia de seguridad de la información para las entidades del sector público español. El ENS tiene por objeto establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de la Administración Pública, y está orientado a la creación de las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos.[48]

La relevancia del ENS para la protección de datos personales en el sector público es directa: las entidades obligadas a cumplir con el Esquema deben adoptar un conjunto de medidas de seguridad clasificadas en función del nivel de seguridad exigido: básico, medio o alto, que se determinará según la categoría del sistema de información. Estas medidas incluyen controles de acceso, cifrado de comunicaciones, registro de actividad, gestión de incidentes y un largo etcétera de requisitos técnicos y organizativos que coinciden, en buena medida, con los exigidos por el RGPD para todos los responsables del tratamiento.

La Directiva NIS2 representa, en el plano europeo, el equivalente del ENS para los sectores esenciales e importantes. Su transposición al ordenamiento español, que debía haberse producido antes del 17 de octubre de 2024, introduce un régimen de gestión de riesgos de ciberseguridad que obliga a las entidades afectadas a adoptar medidas técnicas, operativas y organizativas proporcionadas y adecuadas para gestionar los riesgos que se planteen para la seguridad de las redes y sistemas de información que estas entidades utilizan en sus actividades. Las obligaciones de notificación de incidentes significativos a las autoridades competentes establecidas por la NIS2 son especialmente exigentes en cuanto a plazos; una alerta temprana en 24 horas, una notificación inicial en 72 horas y un informe

[48] Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, BOE núm. 106, de 4 de mayo de 2022 (texto consolidado a 6 de noviembre de 2024) (disponible en https://boe.es/buscar/act.php?id=BOE-A-2022-7191; última consulta: 2 de junio de 2026).

final en un mes, lo que obliga a las entidades afectadas a disponer de capacidades de detección y respuesta muy ágiles.[49]

Capítulo 4. El panorama de amenazas digitales

4.1. Principales ciberamenazas con impacto en datos personales

El panorama de amenazas digitales en Europa ha experimentado una transformación profunda y acelerada en los últimos años. La Agencia de la Unión Europea para la Ciberseguridad (ENISA) publica anualmente un mapa de amenazas el *ENISA Threat Landscape*, que ofrece una visión comprehensiva de los principales vectores de ataque y de su evolución. Los informes de los últimos ejercicios coinciden en señalar un incremento tanto en el número como en la sofisticación de los ataques, con una tendencia creciente hacia la monetización de los datos personales como objetivo primario de muchas de las campañas maliciosas.[50]

Entre las amenazas con mayor impacto en la protección de datos personales, el ransomware ocupa un lugar especialmente destacado. Este tipo de malware cifra los sistemas de la víctima y exige el pago de un rescate para permitir su recuperación; pero, en sus versiones más recientes, añade una amenaza adicional de enorme gravedad: la publicación, filtración o venta de los datos personales exfiltrados si la víctima no accede al pago exigido. De este modo, el ransomware ya no afecta únicamente a la disponibilidad de los sistemas informáticos, sino también a la confidencialidad de la información tratada por la entidad atacada. Los ataques de ransomware a hospitales, administraciones públicas y empresas de servicios esenciales han demostrado ser especialmente dañinos, no solo por las consecuencias que generan para la continuidad del servicio, sino también por el impacto directo sobre la privacidad de miles e incluso millones de personas cuyos datos pueden verse comprometidos. La gravedad de estos

[49] Directiva (UE) 2022/2555 (NIS2), arts. 20-23.
[50] Agencia de la Unión Europea para la Ciberseguridad (ENISA), *ENISA Threat Landscape 2024* (disponible en https://securitydelta.nl/media/com_hsd/report/690/document/ENISA-Threat-Landscape-2024.pdf; última consulta: 2 de junio de 2026).

ataques aumenta cuando la información afectada incluye datos sensibles o especialmente protegidos, pues su exposición puede producir perjuicios difíciles de reparar. Por ello, el ransomware representa uno de los ejemplos más claros de la conexión entre ciberseguridad y protección de datos personales, ya que una brecha técnica puede traducirse rápidamente en una vulneración jurídica de gran alcance.[51]

El *phishing* y sus variantes (*spear phishing, vishing, smishing*) continúan siendo los vectores de entrada más frecuentes en los incidentes de seguridad que afectan a datos personales. Estas técnicas de ingeniería social explotan la confianza de los usuarios para obtener credenciales de acceso o para inducirles a instalar malware, y han evolucionado hasta alcanzar niveles de sofisticación que los hacen difícilmente detectables incluso por usuarios entrenados. El sector financiero es uno de los objetivos predilectos de este tipo de ataques, dada la sensibilidad y el valor económico de los datos que maneja[52]

Las vulnerabilidades en las cadenas de suministro de software representan otro vector de ataque de creciente relevancia. La dependencia de las organizaciones de proveedores de software y servicios digitales crea puntos de fallo que pueden ser explotados por atacantes para comprometer simultáneamente a múltiples víctimas a través de un único proveedor comprometido. Este tipo de ataques, de los que el caso SolarWinds en 2020 es el ejemplo más paradigmático, pone de manifiesto la necesidad de extender las exigencias de ciberseguridad más allá del perímetro propio de cada organización, incluyendo a sus proveedores y subcontratistas.

4.2. Transferencias internacionales de datos y riesgos asociados

El RGPD establece en su Capítulo V un régimen especialmente riguroso para las transferencias de datos personales a países terceros u organizaciones internacionales. El

---

[51] ENISA, *Public Administration Threat Landscape 2024* (disponible en https://www.enisa.europa.eu/sites/default/files/2026-01/ENISA%20Public%20Administration%20TL%202024%20-%20v1.2.pdf; última consulta: 2 de junio de 2026).

[52] ENISA, *Finance Sector Threat Landscape 2024* (disponible en https://www.enisa.europa.eu/sites/default/files/2025-02/Finance%20TL%202024_Final.pdf; última consulta: 2 de junio de 2026).

principio general es que dichas transferencias únicamente puede realizarse cuando el tercer país destinatario garantice un nivel de protección de los datos equivalente al que ofrece la Unión Europea, bien porque así lo haya declarado la Comisión Europea a través de una decisión de adecuación, bien porque el exportador de datos haya adoptado garantías apropiadas, como las cláusulas contractuales tipo aprobadas por la Comisión o se encuentre en alguna de las situaciones excepcionales previstas en el artículo 49 del Reglamento[53]

La historia de las transferencias de datos entre la Unión Europea y los Estados Unidos es, en este contexto, especialmente ilustrativa de las tensiones que genera el diferente nivel de protección que ofrecen los ordenamientos europeo y estadounidense. Tras la invalidación del Safe Harbor por el TJUE en la sentencia Schrems I (C-362/14, de 6 de octubre de 2015), la Comisión Europea y las autoridades estadounidenses negociaron el denominado Privacy Shield, que entró en vigor en 2016 como nuevo marco para las transferencias transatlánticas. Sin embargo, el Privacy Shield fue a su vez declarado inválido por el TJUE en la sentencia Schrems II (C-311/18, de 16 de julio de 2020)[54], al considerar el Tribunal que la legislación estadounidense sobre vigilancia de los servicios de inteligencia no ofrecía a los ciudadanos europeos un nivel de protección equivalente al garantizado en la Unión Europea[55]

La relevancia de la sentencia Schrems II trasciende el ámbito estrictamente técnico de las transferencias internacionales de datos. Su verdadero alcance radica en haber reafirmado que la protección reconocida por el Derecho de la Unión no puede quedar debilitada por el mero hecho de que los datos sean transferidos fuera del territorio europeo. La decisión del Tribunal de Justicia puso de manifiesto que la circulación internacional de información personal exige mecanismos capaces de garantizar un nivel de protección sustancialmente

[53] Reglamento (UE) 2016/679, arts. 44-49. El Capítulo V del RGPD establece el régimen de las transferencias internacionales de datos personales, que solo pueden realizarse si el tercer país de destino ofrece un nivel de protección adecuado o si existen garantías apropiadas.

[54] Sentencia del Tribunal de Justicia de la Unión Europea (Gran Sala) de 16 de julio de 2020, asunto C-311/18, Data Protection Commissioner c. Facebook Ireland Ltd y Maximillian Schrems (Schrems II), ECLI:EU:C:2020:559, por la que se declaró inválida la Decisión de Ejecución (UE) 2016/1250 de la Comisión (Privacy Shield).

[55] Parlamento Europeo (Servicio de Estudios), *Privacy Shield: Adecuación de la protección ofrecida por los EE. UU.* (EPRS_STU(2018)628261_ES), 2018 (disponible en https://www.europarl.europa.eu/RegData/etudes/STUD/2018/628261/EPRS_STU(2018)628261_ES.pdf; última consulta: 2 de junio de 2026).

equivalente al existente dentro de la Unión, especialmente cuando entran en juego sistemas de vigilancia pública o limitaciones al ejercicio efectivo de los derechos de los interesados.[56]

Desde una perspectiva práctica, la doctrina posterior a Schrems II ha puesto de relieve que el problema no se limita a la invalidez de un concreto instrumento de transferencia, sino a la necesidad de revisar el modo en que las organizaciones europeas evalúan los riesgos jurídicos asociados al destino de los datos. La sentencia obliga a abandonar una visión puramente formal del cumplimiento, basada en la existencia de cláusulas contractuales o decisiones administrativas, y exige comprobar si en el país receptor existen garantías efectivas frente al acceso desproporcionado de autoridades públicas. Esta exigencia refuerza la idea central del trabajo: la protección de datos solo es real cuando el marco jurídico se acompaña de condiciones materiales de seguridad y control.[57]

La sentencia Schrems II no puede comprenderse plenamente sin atender al precedente establecido por el Tribunal de Justicia en el asunto Schrems I. En aquella ocasión, el Tribunal cuestionó la suficiencia de las garantías existentes para la transferencia de datos personales desde la Unión Europea hacia Estados Unidos, destacando que la protección de los derechos fundamentales no puede quedar condicionada por mecanismos que no aseguren un nivel de tutela equivalente al reconocido por el ordenamiento europeo. Esta línea jurisprudencial consolidó la idea de que la libre circulación internacional de datos debe ir acompañada de garantías efectivas para los interesados.[58]

[56] García Micó, T. G. y García-Perrote Martínez, I., «Identidad, cesión de datos personales y la decisión Privacy Shield tras la STJUE Schrems II», InDret. Revista para el Análisis del Derecho, núm. 3, 2020, pp. 551-559 (disponible en https://indret.com/identidad-cesion-de-datos-personales-y-la-decision-privacy-shield-tras-la-stjue-schrems-ii/; última consulta: 2 de junio de 2026).
[57] *García Micó, T. G. y García-Perrote Martínez, I., op. cit.*
[58] STJUE de 6 de octubre de 2015, asunto C-362/14, Maximillian Schrems c. Data Protection Commissioner.

PARTE III: RETOS Y OPORTUNIDADES

Capítulo 5. Desafíos emergentes

5.1. Inteligencia artificial y decisiones automatizadas

La inteligencia artificial (IA) representa, en el contexto de la protección de datos personales, un desafío que supera en complejidad y alcance a cualquiera de los que se habían planteado anteriormente. Los sistemas de IA son, por naturaleza, intensivos en datos: necesitan grandes volúmenes de información para ser entrenados, y su funcionamiento genera a su vez nuevos datos que pueden ser objeto de tratamiento. El cruce de datos a escala masiva que hacen posible las técnicas de IA permite elaborar perfiles de las personas de una precisión y profundidad sin precedentes, con implicaciones directas para la privacidad y la autonomía individual.[59]

El RGPD aborda específicamente una de las manifestaciones más problemáticas del uso de la IA en el tratamiento de datos: las decisiones automatizadas y la elaboración de perfiles. El artículo 22 del Reglamento reconoce el derecho de todo interesado a no ser objeto de decisiones basadas únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzcan efectos jurídicos en él o le afecten de modo significativamente análogo. Este derecho tiene excepciones, cuando la decisión sea necesaria para la celebración o ejecución de un contrato, cuando esté autorizada por el Derecho de la Unión o de los Estados miembros, o cuando se base en el consentimiento explícito del interesado—, pero en todos los casos el responsable está obligado a adoptar las medidas adecuadas para salvaguardar los derechos del interesado, incluida la posibilidad de obtener intervención humana, de expresar su punto de vista y de impugnar la decisión[60]

[59] Masbernat, P. y Pasquino, V., «Inteligencia Artificial y su problemático impacto en el Derecho», *Revista de Educación y Derecho*, núm. 28, 2023 (disponible en https://dialnet.unirioja.es/descarga/articulo/9187372.pdf; última consulta: 2 de junio de 2026).

[60] Reglamento (UE) 2016/679, art. 22. El precepto reconoce el derecho a no ser objeto de decisiones basadas únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzcan efectos jurídicos en el interesado o le afecten significativamente de modo similar.

El Reglamento de Inteligencia Artificial de la Unión Europea (AI Act), adoptado en junio de 2024, completa el marco normativo europeo en esta materia. El AI Act establece una clasificación de los sistemas de IA en función de su nivel de riesgo: inaceptable, alto, limitado y mínimo, y establece requisitos más o menos exigentes según esa clasificación. Los sistemas de IA de riesgo inaceptable quedan prohibidos, entre ellos la identificación biométrica remota en espacios de acceso público con fines represivos, salvo excepciones muy tasadas—, la puntuación social y los sistemas que manipulen el comportamiento de las personas de forma subliminal. Los sistemas de IA de alto riesgo, entre los que se incluyen muchos de los que se utilizan en la toma de decisiones en sectores como el empleo, la educación, la justicia o la atención sanitaria, están sujetos a requisitos de transparencia, supervisión humana, solidez y precisión, y documentación que se articulan de forma complementaria con las obligaciones del RGPD.[61]

La inteligencia artificial no plantea únicamente problemas técnicos de funcionamiento, sino también interrogantes jurídicos de fondo. Su utilización en ámbitos cada vez más relevantes de la vida social obliga a repensar categorías tradicionales como la responsabilidad, la transparencia, la autonomía de la voluntad o la igualdad de trato. Cuando una decisión que afecta a una persona se apoya en sistemas automatizados difíciles de comprender, el problema no es solo si el resultado es correcto, sino si el procedimiento seguido resulta compatible con las exigencias propias de un Estado de Derecho.[62]

A los problemas de transparencia y control se añade una cuestión especialmente relevante: la atribución de responsabilidad cuando el uso de sistemas de inteligencia artificial provoca daños. En estos casos, la dificultad no reside únicamente en identificar el resultado

[61] Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial (Reglamento de Inteligencia Artificial o AI Act), DOUE L, de 12 de julio de 2024 (disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=OJ%3AL_202401689; última consulta: 2 de junio de 2026).

[62] MASBERNAT, P. y PASQUINO, V., «Inteligencia Artificial y su problemático impacto en el Derecho», Revista de Educación y Derecho, núm. 28, 2023.

lesivo, sino en determinar quién debe responder por él: el desarrollador del sistema, quien lo comercializa, quien lo utiliza o la organización que adopta la decisión final. Esta complejidad se acentúa cuando el sistema funciona con cierto grado de autonomía o cuando sus procesos internos no resultan fácilmente explicables, lo que obliga al Derecho a adaptar sus criterios tradicionales de imputación y diligencia.[63]

La intersección entre el AI Act y el RGPD plantea, sin embargo, importantes cuestiones de articulación que la doctrina todavía está explorando. Los principios de protección de datos desde el diseño y por defecto, la evaluación de impacto en la protección de datos o la exigencia de transparencia encuentran su correlato en el AI Act en los requisitos de documentación técnica, transparencia para los usuarios e intervención humana; pero los conceptos no son siempre equivalentes y las obligaciones pueden no coincidir exactamente. Esta superposición normativa exige de los responsables del tratamiento y de los desplegadores de sistemas de IA un esfuerzo de coordinación y cumplimiento conjunto que, en la práctica, resulta de notable complejidad.

La capacidad de recopilar y procesar cantidades masivas de información ha transformado profundamente el modo en que se toman decisiones sobre las personas. A diferencia de los tratamientos tradicionales, los sistemas basados en grandes volúmenes de datos permiten identificar patrones de comportamiento, anticipar preferencias e incluso realizar inferencias sobre aspectos que el propio individuo nunca ha comunicado expresamente. Esta realidad incrementa el riesgo de que se adopten decisiones basadas en perfiles digitales construidos a partir de múltiples fuentes de información, lo que plantea importantes desafíos para los principios de transparencia, minimización de datos y control efectivo por parte del interesado[64]

---

[63] MORENO MARTÍNEZ, J. A. y FEMENÍA LÓPEZ, P. J. (coords.), *Inteligencia artificial y derecho de daños: cuestiones actuales. Acorde al Reglamento (UE) 2024/1689*, Dykinson, Madrid, 2024.

[64] GIL GONZÁLEZ, E., *Big data, privacidad y protección de datos*, Agencia Española de Protección de Datos y Agencia Estatal Boletín Oficial del Estado, Madrid, 2016.

Ante los riesgos derivados del tratamiento automatizado de información, la protección de los derechos fundamentales no puede limitarse a mecanismos correctivos una vez producido el daño. Resulta necesario incorporar garantías jurídicas desde las fases iniciales de diseño de los sistemas tecnológicos, de forma que la protección de datos, la transparencia y la supervisión humana constituyan elementos integrados en la propia arquitectura de las herramientas digitales. Esta aproximación preventiva adquiere una relevancia especial en los sistemas de inteligencia artificial, cuya complejidad puede dificultar la identificación de sesgos, errores o decisiones potencialmente discriminatorias[65].

Entre las categorías de información que requieren una protección especialmente intensa destacan los datos relativos a la salud. Su tratamiento puede revelar aspectos extremadamente sensibles de la vida de una persona y generar consecuencias relevantes tanto en el ámbito profesional como en el social o familiar. Por ello, la jurisprudencia europea ha insistido en que la confidencialidad de esta información constituye un presupuesto esencial para preservar la confianza de los ciudadanos en los sistemas sanitarios y para garantizar el respeto efectivo de la vida privada.[66]

La evolución tecnológica obliga a superar una visión excesivamente rígida del conflicto entre innovación y protección de los derechos fundamentales. Las tecnologías digitales pueden aportar beneficios relevantes en ámbitos como la investigación científica, la prestación de servicios públicos, la medicina personalizada o la eficiencia empresarial, pero esos avances no eliminan la necesidad de preservar espacios de autonomía individual. Precisamente por ello, el reto jurídico no consiste en frenar el desarrollo tecnológico, sino en asegurar que este se produzca dentro de un marco compatible con la dignidad, la privacidad y la libertad de las personas.[67]

---

[65] MARTÍNEZ MARTÍNEZ, R., «Inteligencia artificial desde el diseño: retos y estrategias para el cumplimiento normativo», *Revista Catalana de Dret Públic*, núm. 58, 2019, pp. 64-81.

[66] STEDH de 25 de febrero de 1997, *Z. c. Finlandia*, demanda n.º 22009/93.

[67] PARLAMENTO EUROPEO, SERVICIO DE ESTUDIOS, *El derecho al respeto de la vida privada: los retos digitales, una perspectiva de Derecho comparado*, Consejo de Europa, 2018.

Esta tensión se aprecia con especial intensidad en el ámbito de la inteligencia artificial. Los sistemas automatizados pueden facilitar la toma de decisiones y mejorar la gestión de grandes volúmenes de información, pero también pueden generar riesgos vinculados a la opacidad, la discriminación algorítmica y la dificultad para comprender los criterios utilizados en una decisión que afecta a una persona concreta. En este contexto, el problema jurídico no se limita al resultado final, sino que alcanza también al procedimiento seguido para obtenerlo y a la posibilidad real de controlarlo.[68]

Por ello, la respuesta jurídica más adecuada parece orientarse hacia un modelo preventivo. La protección de los derechos no puede depender únicamente de mecanismos posteriores de reclamación o reparación, sino que debe incorporarse desde las fases iniciales de diseño, desarrollo e implementación de los sistemas tecnológicos. Esta lógica conecta directamente con la protección de datos desde el diseño y por defecto, y permite entender la privacidad como un elemento que debe integrarse en la arquitectura misma de las herramientas digitales, no como una corrección añadida cuando el riesgo ya se ha materializado.[69]

A ello se suma la necesidad de adaptar las categorías tradicionales de responsabilidad a un entorno tecnológico cada vez más complejo y descentralizado. Cuando intervienen desarrolladores, proveedores, usuarios profesionales y organizaciones que adoptan decisiones basadas en sistemas automatizados, no siempre resulta sencillo determinar quién debe responder por un eventual daño ni en qué medida puede imputarse dicho daño a cada uno de los sujetos implicados. Esta dificultad se acentúa cuando las decisiones no proceden de una actuación humana directa, sino del funcionamiento de herramientas tecnológicas que procesan grandes cantidades de información y generan resultados que pueden influir de

[68]MASBERNAT, P. y PASQUINO, V., «Inteligencia Artificial y su problemático impacto en el Derecho», op. cit.

[69]MARTÍNEZ MARTÍNEZ, R., «Inteligencia artificial desde el diseño: retos y estrategias para el cumplimiento normativo», op. cit., pp. 64-81.

manera relevante en la vida de las personas. En este contexto, los esquemas clásicos de responsabilidad, construidos sobre relaciones causales más simples y fácilmente identificables, pueden resultar insuficientes para afrontar supuestos en los que concurren múltiples actores, fases técnicas distintas y diferentes niveles de control sobre el sistema utilizado. Por ello, resulta necesario reforzar los deberes de diligencia, documentación y supervisión a lo largo de todo el ciclo de vida de estas tecnologías, desde su diseño y desarrollo hasta su implantación y uso efectivo. Esta exigencia adquiere especial importancia en aquellos supuestos en los que el empleo de tecnologías avanzadas puede afectar a derechos fundamentales o producir consecuencias significativas para las personas, ya que en tales casos no basta con confiar en el funcionamiento automático del sistema. Es preciso garantizar que existan mecanismos de control, trazabilidad y revisión que permitan identificar riesgos, prevenir daños y, en su caso, determinar responsabilidades de manera adecuada..[70]

Con todo ello, los retos futuros no pasan por elegir entre innovación tecnológica o protección de derechos fundamentales, sino por construir un modelo capaz de compatibilizar ambos objetivos. La consolidación de un entorno digital seguro, transparente y respetuoso con la dignidad humana constituye una condición necesaria para aprovechar las oportunidades que ofrecen las nuevas tecnologías sin renunciar a los valores que sustentan el Estado de Derecho.

5.2. El derecho al olvido en la era del Big Data

El derecho al olvido es, quizás, la manifestación más visible y mediáticamente reconocida del conjunto de derechos que el ordenamiento europeo reconoce a los titulares de datos personales. Su configuración jurídica actual es el resultado de la combinación de la construcción jurisprudencial del TJUE —iniciada con la sentencia Google Spain de 2014— y de su codificación en el artículo 17 del RGPD como "derecho de supresión". Sin embargo, la

[70] MORENO MARTÍNEZ, J. A. y FEMENÍA LÓPEZ, P. J. (coords.), *Inteligencia artificial y derecho de daños: cuestiones actuales*, op. cit.

aplicación de este derecho en la era del Big Data y de la inteligencia artificial plantea desafíos que la norma vigente no resuelve plenamente.[71]

La sentencia Google Spain estableció que el interesado puede exigir que información veraz y lícitamente publicada sobre él sea retirada de los resultados de un motor de búsqueda cuando, atendiendo a las circunstancias del caso y en particular al tiempo transcurrido, esa información ya no sea relevante, adecuada o proporcional a los fines del tratamiento. El Tribunal realizó una ponderación entre el derecho a la protección de datos del interesado y el interés del público en acceder a esa información, afirmando que, como regla general, los primeros prevalecen sobre el segundo, sin perjuicio de que pueda existir interés público prevalente en ciertos supuestos, como cuando el interesado desempeña un papel relevante en la vida pública[72]

El RGPD recogió y sistematizó ese derecho en su artículo 17, estableciendo de manera detallada las condiciones en las que el interesado puede solicitar la supresión de sus datos personales y los límites que pueden impedir o restringir el ejercicio de dicho derecho. De este modo, el derecho de supresión no se configura como una facultad absoluta, sino como un derecho sometido a una necesaria ponderación con otros intereses y derechos igualmente protegidos por el ordenamiento jurídico. Las excepciones más relevantes son las que protegen el ejercicio de la libertad de expresión e información, el cumplimiento de una obligación legal, el interés público en el ámbito de la salud pública, los fines de archivo en interés público, de investigación científica o histórica o estadística, y la formulación, el ejercicio o la defensa de reclamaciones. Esta enumeración demuestra que el legislador europeo ha tratado de evitar que el derecho de supresión pueda utilizarse de manera desproporcionada o contraria a otros valores jurídicos esenciales. Por ello, la aplicación

[71] Bouzas Mendes, R. E., *op. cit.*, pp. 113-148. El autor analiza la evolución del derecho al olvido desde la sentencia *Google Spain* hasta el RGPD, y reflexiona sobre los límites y tensiones que este derecho plantea en la era del Big Data.

[72]Sentencia del Tribunal de Justicia de la Unión Europea de 13 de mayo de 2014, asunto C-131/12, *Google Spain*, apartados 80-99. El Tribunal analizó detalladamente las condiciones en las que el interesado puede solicitar la retirada de enlaces a información sobre él de los resultados de un motor de búsqueda, ponderando ese derecho con la libertad de información y el interés público.

práctica del artículo 17 exige valorar no solo el interés individual del afectado en que sus datos sean eliminados, sino también la posible existencia de razones legítimas que justifiquen su conservación o difusión. La ponderación entre el derecho de supresión y estas excepciones es, en muchos casos, extraordinariamente compleja, especialmente en el entorno digital, donde la información puede difundirse con rapidez, permanecer accesible durante largos periodos de tiempo y afectar simultáneamente a intereses individuales y colectivos. Por esta razón, cada solicitud debe analizarse caso por caso, atendiendo a las circunstancias concretas del tratamiento, a la naturaleza de la información afectada, a la finalidad para la que se conserva y al impacto que su eliminación o mantenimiento puede tener sobre otros derechos. En este contexto, las plataformas digitales desempeñan un papel particularmente relevante, pues son con frecuencia quienes reciben y tramitan estas solicitudes, aunque su actuación debe quedar sometida a la supervisión de las autoridades de control competentes para garantizar una aplicación equilibrada y conforme al RGPD.[73]

En la era del Big Data, el derecho al olvido enfrenta desafíos adicionales que la regulación actual todavía no aborda satisfactoriamente. En primer lugar, la lógica acumulativa y combinatoria de los grandes sistemas de datos hace que la simple supresión de un dato de un sistema concreto no garantice que la información deje de ser accesible o utilizable: si el mismo dato ha sido replicado en múltiples bases de datos, cedido a terceros o utilizado para entrenar modelos de IA, la supresión en origen puede resultar insuficiente. En segundo lugar, la aplicación del derecho al olvido a los modelos de aprendizaje automático en los que los datos personales no están almacenados como tales sino incorporados a los parámetros del modelo plantea problemas técnicos de difícil solución que la doctrina especializada denomina *machine unlearning*.

[73] Reglamento (UE) 2016/679, art. 17. El precepto reconoce el derecho de supresión o derecho al olvido, estableciendo las condiciones en las que el interesado puede solicitar la supresión de sus datos personales, así como las excepciones a ese derecho por razones de interés público, ejercicio de la libertad de expresión o interés científico, histórico o estadístico.

Capítulo 6. Propuestas y reflexión final

6.1. La búsqueda de una cultura de privacidad proactiva

La construcción de una cultura de privacidad proactiva es, probablemente, el reto más transversal y de más largo plazo que plantea el entorno digital contemporáneo. La existencia de una normativa técnicamente avanzada como el RGPD es condición necesaria pero no suficiente para garantizar la efectividad del derecho a la protección de datos. Es igualmente necesario que los operadores jurídicos, los responsables y encargados del tratamiento, los profesionales de la tecnología y los propios ciudadanos interioricen los valores que subyacen a esa normativa y los trasladen a sus prácticas cotidianas.[74]

El concepto de privacy by design, desarrollado por Ann Cavoukian en la década de los noventa y recogido por el RGPD en su artículo 25, expresa bien esta aspiración: la privacidad no debe ser un añadido externo que se aplica a los sistemas una vez diseñados, sino un valor incorporado desde el inicio en la concepción de cualquier sistema, proceso u organización que implique el tratamiento de datos personales. Esta aspiración requiere, entre otras cosas, que los profesionales de la tecnología tengan formación en materia de privacidad, que los juristas entiendan los aspectos técnicos de los sistemas que asesoran, y que los directivos de las organizaciones perciban la protección de datos no como una carga regulatoria sino como un elemento de confianza y de valor añadido.

La noción de privacidad proactiva implica también una actitud preventiva frente a los riesgos, en lugar de reactiva. El análisis de riesgos, la evaluación de impacto y la revisión periódica de las medidas de seguridad son manifestaciones concretas de esa actitud. No se trata de esperar a que se produzca una brecha de seguridad para tomar medidas, sino de anticiparse a los riesgos y neutralizarlos antes de que se materialicen. Esta lógica preventiva es coherente con la filosofía general del RGPD, que en su considerando 83 afirma que el

[74] Agencia Española de Protección de Datos, *Guía de Privacidad desde el Diseño…*, *op. cit.*, pp. 32-33.

responsable del tratamiento debe evaluar los riesgos inherentes al tratamiento y aplicar medidas para mitigarlos.[75]

La consolidación y formación de una sociedad plenamente digital exige superar una concepción puramente reactiva de la protección de datos y de la ciberseguridad. La creciente integración de tecnologías avanzadas en ámbitos tan diversos como la educación, la sanidad, el trabajo o la administración pública demuestra que los riesgos asociados al tratamiento de información personal no pueden afrontarse únicamente mediante mecanismos sancionadores. Resulta necesario fomentar una cultura preventiva basada en la responsabilidad, la formación continua y la incorporación de consideraciones éticas en el desarrollo y utilización de las nuevas tecnologías. Solo desde esta perspectiva puede garantizarse que la innovación tecnológica se desarrolle de forma compatible con la protección efectiva de los derechos fundamentales.[76]

6.2. Propuestas de mejora normativa (lege ferenda)

El análisis del marco normativo vigente y de los desafíos emergentes permite identificar algunas líneas de reforma que merecen ser consideradas por el legislador europeo y nacional. Estas propuestas no pretenden agotar el debate, sino ofrecer algunas reflexiones fundamentadas en el estudio realizado.[77]

En primer lugar, la articulación entre el RGPD y el AI Act requiere un esfuerzo de clarificación normativa que reduzca las zonas de incertidumbre y de posible solapamiento o contradicción entre ambos instrumentos. La Comisión Europea debería desarrollar orientaciones específicas que expliquen cómo deben interpretarse y aplicarse conjuntamente

[75] Casas Baamonde, M. E. (coord.), *op. cit.*, pp. 11-15. La autora destaca que la defensa de los derechos fundamentales, en concreto del derecho a la protección de datos, es el fundamento de la democracia, y que sin privacidad y libertad de las personas no hay democracia.
[76] BURZACO SAMPER, M. y CORRIPIO GIL-DELGADO, J., en DOBRATINICH, G. A. (dir.), *Derecho y nuevas tecnologías*, La Ley, Buenos Aires, 2021.
[77] Masbernat, P. y Pasquino, V., *op. cit.*, pp. 15-18. Los autores reflexionan sobre la necesidad de adaptar las categorías jurídicas tradicionales a los nuevos retos planteados por la IA y concluyen que nos encontramos ante un cambio de paradigma que exige una profunda revisión de las teorías jurídicas vigentes.

ambos reglamentos, en particular en lo relativo a las evaluaciones de impacto, la transparencia y la supervisión humana. La doctrina del "machine unlearning" como la capacidad técnica de "desaprender" los datos de un interesado que ejerce su derecho de supresión en el contexto de modelos de IA, que necesita ser abordada de forma explícita en futuras orientaciones del CEPD o en revisiones del propio RGPD.[78]

En segundo lugar, el régimen del consentimiento para el tratamiento de datos personales con fines publicitarios en las plataformas digitales necesita ser reforzado. La experiencia de los años transcurridos desde la aplicación del RGPD ha evidenciado que el consentimiento obtenido a través de complejos "banners" de cookies no cumple, en la mayor parte de los casos, los requisitos de libertad, información, especificidad e inequivocidad que exige el Reglamento. Una reforma que simplifique y haga más transparente el ejercicio del consentimiento, limitando la utilización del legitimate interest como alternativa en contextos de tratamiento con fines de publicidad comportamental, contribuiría significativamente a la efectividad del derecho a la protección de datos.[79]

En tercer lugar, es necesario reforzar las capacidades de cumplimiento de las pequeñas y medianas empresas (pymes), que en muchos casos carecen de los recursos humanos y económicos necesarios para implementar todos los requisitos del RGPD. Sin cuestionar el nivel de garantías que ofrece el Reglamento, sería conveniente desarrollar mecanismos de apoyo específicos —como programas de certificación accesibles, modelos simplificados de cumplimiento o asesoramiento subsidiado— que faciliten a las pymes el cumplimiento de sus obligaciones en materia de protección de datos.

En cuarto lugar, la transposición de la Directiva NIS2 en España debe aprovecharse para mejorar la coordinación entre las autoridades competentes en materia de ciberseguridad; principalmente el Centro Criptológico Nacional (CCN) y el Instituto Nacional de Ciberseguridad (INCIBE) y la AEPD. La ciberseguridad y la protección de datos son, como

[78] Reglamento (UE) 2024/1689 (AI Act), arts. 9-13.
[79] Polo Roca, A., *op. cit.*, pp. 188-192. El autor propone, entre otras mejoras, reforzar las garantías del consentimiento

se ha argumentado a lo largo de este trabajo, dos caras de una misma moneda, y la ausencia de coordinación entre las autoridades responsables de cada uno de estos ámbitos puede generar duplicidades, incoherencias o vacíos de supervisión que redunden en perjuicio de los ciudadanos.

CONCLUSIONES

El recorrido realizado a lo largo de este Trabajo de Fin de Grado permite extraer un conjunto de conclusiones que, lejos de cerrar el debate, pretenden contribuir a su enriquecimiento y a la comprensión de un fenómeno jurídico de enorme relevancia en las sociedades contemporáneas. La progresiva digitalización de la actividad humana ha convertido la privacidad y la protección de los datos personales en elementos esenciales para la preservación de los derechos fundamentales, planteando retos de gran complejidad para el Derecho, las instituciones públicas y los operadores privados.

Primera. La privacidad constituye un derecho fundamental de profunda tradición filosófica y jurídica, estrechamente vinculado a la dignidad humana, la libertad individual y la autonomía personal. Su evolución histórica demuestra la capacidad de adaptación del Derecho ante las transformaciones sociales y tecnológicas. Desde la formulación clásica del *right to be let alone* por Warren y Brandeis hasta la consolidación de la teoría de la autodeterminación informativa desarrollada por la jurisprudencia europea, puede observarse una ampliación progresiva de la protección jurídica de la persona frente a nuevas formas de injerencia. En el ordenamiento español, el artículo 18 de la Constitución proporciona una sólida base para la tutela de estos derechos, mientras que el reconocimiento autónomo del derecho a la protección de datos en el artículo 8 de la Carta de Derechos Fundamentales de la Unión Europea ha supuesto uno de los avances más significativos en la construcción del modelo europeo de protección de los derechos digitales. Este reconocimiento no solo tiene relevancia teórica, sino que se proyecta directamente sobre la vida cotidiana de millones de ciudadanos, otorgándoles instrumentos efectivos para controlar el uso de su información personal.

Segunda. El sistema europeo de protección de datos, articulado principalmente a través del Reglamento General de Protección de Datos y complementado en España por la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales, representa actualmente el modelo normativo más completo y garantista existente a nivel internacional. Los principios de licitud, lealtad, transparencia, minimización, limitación de la finalidad, exactitud, integridad y confidencialidad constituyen auténticos pilares sobre los que descansa la protección jurídica de la información personal. Del mismo modo, el amplio catálogo de derechos reconocidos a los interesados refuerza la posición del ciudadano frente a quienes tratan sus datos. Especial importancia reviste el principio de responsabilidad proactiva, que ha transformado profundamente la lógica tradicional del cumplimiento normativo, obligando a las organizaciones a integrar la protección de datos en todos sus procesos internos y a demostrar de forma continua el respeto a las obligaciones legales. Este cambio de paradigma refleja una concepción moderna de la regulación, basada no solo en la reacción frente a las infracciones, sino también en la prevención y gestión constante de los riesgos.

Tercera. La ciberseguridad debe ser entendida como una verdadera garantía jurídica del derecho fundamental a la protección de datos y no únicamente como una cuestión de naturaleza tecnológica. El análisis realizado pone de manifiesto que la efectividad de los derechos reconocidos por el RGPD depende en gran medida de la existencia de medidas técnicas y organizativas adecuadas que permitan preservar la confidencialidad, integridad y disponibilidad de la información. La obligación de implantar medidas de seguridad adecuadas, la gestión de brechas de seguridad, la protección de datos desde el diseño y por defecto, así como los mecanismos previstos por el Esquema Nacional de Seguridad y la Directiva NIS2, evidencian que la seguridad informática ha adquirido una dimensión plenamente jurídica. En consecuencia, la vulneración de estas obligaciones puede generar importantes consecuencias legales, económicas y reputacionales para las organizaciones responsables del tratamiento. La creciente sofisticación de los ciberataques demuestra que la protección de datos y la ciberseguridad son hoy realidades inseparables que deben abordarse de manera conjunta.

Cuarta. Las tecnologías emergentes, especialmente la inteligencia artificial y los sistemas de tratamiento masivo de información, constituyen uno de los mayores desafíos para el futuro de la protección de datos. La capacidad de estas herramientas para recopilar, procesar y analizar grandes volúmenes de información plantea cuestiones complejas relacionadas con la transparencia algorítmica, la elaboración de perfiles, la toma automatizada de decisiones y la posible aparición de sesgos discriminatorios. Aunque el RGPD proporciona mecanismos relevantes para afrontar algunos de estos problemas, resulta evidente que muchas de las cuestiones planteadas por la inteligencia artificial exceden el marco regulatorio originalmente previsto. La aprobación del Reglamento Europeo de Inteligencia Artificial representa un paso importante en esta dirección, pero su aplicación práctica exigirá una intensa labor interpretativa por parte de los tribunales, las autoridades de control y la doctrina jurídica. La evolución tecnológica continuará generando situaciones inéditas que requerirán respuestas normativas dinámicas y flexibles.

Quinta. Las propuestas de mejora formuladas a lo largo del trabajo ponen de manifiesto que la consolidación de una protección efectiva de los datos personales requiere no solo reformas legislativas, sino también un cambio cultural profundo. La clarificación de la relación entre el RGPD y el *AI Act*, el fortalecimiento de los mecanismos de consentimiento, el apoyo a pequeñas y medianas empresas en materia de cumplimiento normativo y el refuerzo de la cooperación entre autoridades constituyen algunas de las líneas de actuación más relevantes para los próximos años. Sin embargo, ninguna reforma será plenamente eficaz si no va acompañada de una mayor concienciación social sobre el valor de la privacidad y sobre la importancia de la protección de los datos personales como elemento esencial para el ejercicio de los derechos fundamentales.

Sexta. Como conclusión general, puede afirmarse que la privacidad y la protección de datos personales se han convertido en una de las cuestiones centrales del constitucionalismo contemporáneo. Lejos de constituir una materia exclusivamente técnica o administrativa, afectan directamente a la libertad, la igualdad, la dignidad humana y la calidad democrática de nuestras sociedades. El gran desafío jurídico del siglo XXI consiste en garantizar que el

desarrollo tecnológico continúe generando progreso económico y social sin erosionar los derechos fundamentales que constituyen la base del Estado de Derecho. Alcanzar este equilibrio será una tarea compleja y permanente, pero también imprescindible para asegurar que la transformación digital se produzca al servicio de las personas y no a costa de ellas. Este trabajo ha pretendido aportar una reflexión crítica sobre esta cuestión, consciente de que la evolución tecnológica seguirá planteando nuevos retos y que el debate jurídico en torno a la privacidad y la protección de datos está todavía lejos de concluir.

BIBLIOGRAFÍA Y FUENTES

1. LEGISLACIÓN

Constitución Española, BOE núm. 311, de 29 de diciembre de 1978.

Carta de los Derechos Fundamentales de la Unión Europea, DOUE C 326, de 26 de octubre de 2012.

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 (Reglamento General de Protección de Datos), DOUE L 119, de 4 de mayo de 2016.

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, BOE núm. 294, de 6 de diciembre de 2018.

Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, BOE núm. 106, de 4 de mayo de 2022.

Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión (Directiva NIS2), DOUE L 333, de 27 de diciembre de 2022.

Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial (Reglamento de Inteligencia Artificial), DOUE L, de 12 de julio de 2024.

2. JURISPRUDENCIA

Tribunal Constitucional (España)

Sentencia del Tribunal Constitucional (Pleno) núm. 292/2000, de 30 de noviembre, FF.JJ. 6 y 7 (recurso de inconstitucionalidad núm. 1463/2000), BOE núm. 4, de 4 de enero de 2001.

Tribunal Constitucional Federal de Alemania (Bundesverfassungsgericht)

Sentencia de 15 de diciembre de 1983, asunto 1 BvR 209/83 y acumulados (Sentencia del Censo, *Volkszählungsurteil*), BVerfGE 65, 1.

Tribunal de Justicia de la Unión Europea

Sentencia de 8 de abril de 2014, asuntos acumulados C-293/12 y C-594/12, *Digital Rights Ireland Ltd*.

Sentencia de 13 de mayo de 2014, asunto C-131/12, *Google Spain SL y Google Inc. c. Agencia Española de Protección de Datos (AEPD) y Mario Costeja González*(disponible en https://www.abogacia.es/wp-content/uploads/2014/05/Sentencia-131-12-TJUE-derecho-al-olvido.pdf; última consulta: 2 de junio de 2026).

Sentencia de 6 de octubre de 2015, asunto C-362/14, *Maximillian Schrems c. Data Protection Commissioner*.

Sentencia (Gran Sala) de 16 de julio de 2020, asunto C-311/18, *Data Protection Commissioner c. Facebook Ireland Ltd y Maximillian Schrems* (Schrems II), ECLI:EU:C:2020:559.

Tribunal Europeo de Derechos Humanos

Sentencia de 25 de febrero de 1997, asunto *Z c. Finlandia*, demanda núm. 22009/93.

Sentencia (Gran Sala) de 7 de febrero de 2012, asunto *Von Hannover c. Alemania (n.º 2)*, demandas núms. 40660/08 y 60641/08 (disponible en https://globalfreedomofexpression.columbia.edu/cases/von-hannover-v-germany-no-2/?lang=es; última consulta: 2 de junio de 2026)

3. OBRAS DOCTRINALES

Bouzas Mendes, R. E., «El reto de la privacidad en la era de internet», *Revista de Derecho UNED*, núm. 31, 2023, pp. 113-148.

Burzaco Samper, M. y Corripio Gil-Delgado, J., en Dobratinich, G. A. (dir.), *Derecho y nuevas tecnologías*, La Ley, Buenos Aires, 2021,.

Casas Baamonde, M. E. (coord.), *El derecho a la protección de datos personales en la sociedad digital*, Fundación Ramón Areces, Madrid, 2020.

De la Quadra-Salcedo Fernández del Castillo, T. y Piñar Mañas, J. L. (dirs.), *Sociedad digital y Derecho*, Boletín Oficial del Estado, Ministerio de Industria, Comercio y Turismo y Red.es, Madrid, 2018.

García Micó, T. G. y García-Perrote Martínez, I., «Identidad, cesión de datos personales y la decisión Privacy Shield tras la STJUE Schrems II», *InDret. Revista*

para el Análisis del Derecho, núm. 3, 2020, pp. 551-559 (disponible en https://indret.com/identidad-cesion-de-datos-personales-y-la-decision-privacy-shield-tras-la-stjue-schrems-ii/; última consulta: 8 de junio de 2026).

GIL GONZÁLEZ, E., *Big data, privacidad y protección de datos*, Agencia Española de Protección de Datos y Agencia Estatal Boletín Oficial del Estado, Madrid, 2016.

HERNÁNDEZ LÓPEZ, J. M., «Protección de datos, intimidad y acceso a la información pública. Ponderación y proporcionalidad», *Revista Canaria de Administración Pública*, núm. 5, 2025, pp. 79-105.

MARTÍNEZ DE PISÓN, J., «El derecho a la intimidad: de la configuración inicial a los últimos desarrollos en la jurisprudencia constitucional», *Anuario de Filosofía del Derecho*, vol. XXXII, 2016, pp. 409-430.

MARTÍNEZ MARTÍNEZ, R., «Inteligencia artificial desde el diseño: retos y estrategias para el cumplimiento normativo», *Revista Catalana de Dret Públic*, núm. 58, 2019, pp. 64-81.

MASBERNAT, P. y PASQUINO, V., «Inteligencia Artificial y su problemático impacto en el Derecho», *Revista de Educación y Derecho*, núm. 28, 2023,.

MORENO MARTÍNEZ, J. A. y FEMENÍA LÓPEZ, P. J. (coords.), *Inteligencia artificial y derecho de daños: cuestiones actuales. Acorde al Reglamento (UE) 2024/1689*, Dykinson, Madrid, 2024.

PIÑAR MAÑAS, J. L., «El derecho a la protección de datos de carácter personal en la jurisprudencia del Tribunal de Justicia de las Comunidades Europeas», *Cuadernos de Derecho Público*, núms. 19-20, 2003, pp. 45-90.

PIÑAR MAÑAS, J. L., «¿Existe privacidad?», en *Lecturas sobre privacidad y protección de datos*, Instituto Federal de Acceso a la Información y Protección de Datos, México, 2010.

PIÑAR MAÑAS, J. L., «Derecho e innovación. Privacidad y otros derechos en la sociedad digital», en CASAS BAAMONDE, M. E. (coord.), *El derecho a la protección de datos personales en la sociedad digital*, Fundación Ramón Areces, Madrid, 2020, pp. 39-63.

POLO ROCA, A., «El derecho a la protección de datos personales y su reflejo en el consentimiento del interesado», *Revista de Derecho Político*, núm. 108, 2020, pp. 165-194.

SALDAÑA, M. N., «"The Right to Privacy". La génesis de la protección de la privacidad en el sistema constitucional norteamericano: el centenario legado de Warren y Brandeis», *Revista de Derecho Político*, núm. 85, 2012, pp. 195-240.

WARREN, S. D. y BRANDEIS, L. D., «The Right to Privacy», *Harvard Law Review*, vol. IV, núm. 5, 1890, pp. 193-220.

4. RECURSOS DE INTERNET Y FUENTES INSTITUCIONALES

Agencia de la Unión Europea para la Ciberseguridad (ENISA), *ENISA Threat Landscape 2024*, 2024 (disponible en https://securitydelta.nl/media/com_hsd/report/690/document/ENISA-Threat-Landscape-2024.pdf; última consulta: 2 de junio de 2026).

Agencia de la Unión Europea para la Ciberseguridad (ENISA), *Finance Sector Threat Landscape 2024*, 2024 (disponible en https://www.enisa.europa.eu/sites/default/files/2025-02/Finance%20TL%202024_Final.pdf; última consulta: 2 de junio de 2026).

Agencia de la Unión Europea para la Ciberseguridad (ENISA), *Public Administration Threat Landscape 2024* (v1.2), 2024 (disponible en https://www.enisa.europa.eu/sites/default/files/2026-01/ENISA%20Public%20Administration%20TL%202024%20-%20v1.2.pdf; última consulta: 2 de junio de 2026).

Agencia de los Derechos Fundamentales de la Unión Europea y Consejo de Europa, *Manual de legislación europea en materia de protección de datos*, Oficina de Publicaciones de la Unión Europea, Luxemburgo, 2018.

Agencia Española de Protección de Datos, *Guía de Privacidad desde el Diseño*, octubre de 2019 (disponible en https://www.aepd.es/guias/guia-privacidad-desde-diseno.pdf; última consulta: 2 de junio de 2026).

Agencia Española de Protección de Datos, *Guía para la notificación de brechas de datos personales*, junio de 2021 (disponible en https://www.aepd.es/guias/guia-brechas-seguridad.pdf; última consulta: 2 de junio de 2026).

Comité Europeo de Protección de Datos, *Marco legal del CEPD* (disponible en https://www.edpb.europa.eu/about-edpb/about-edpb/legal-framework_es; última consulta: 2 de junio de 2026).

Parlamento Europeo (Servicio de Estudios), *El derecho al respeto de la vida privada: los retos digitales, una perspectiva de Derecho comparado*, Consejo de Europa, 2018.

Parlamento Europeo (Servicio de Estudios), *Privacy Shield: Adecuación de la protección ofrecida por los EE. UU.* (EPRS_STU(2018)628261_ES), 2018 (disponible en https://www.europarl.europa.eu/RegData/etudes/STUD/2018/628261/EPRS_STU(2018)628261_ES.pdf; última consulta: 2 de junio de 2026).