Documentación Administrativa, número 15, diciembre de 2025
Sección: ARTÍCULOS
Recibido: 22-10-2025
Modificado: 21-12-2025
Aceptado: 08-01-2026
Publicado: 22-01-2026
ISSN: 1989-8983 – DOI: https://doi.org/10.24965/da.11601
Páginas: 77-91

Referencia: Caja Moya, C. y Quiroga Rodríguez, E. (2025). La intimidad de los ciudadanos en la sala de espera: hacia una directiva europea de protección física de datos personales. *Documentación Administrativa*, 15, 77-91. https://doi.org/10.24965/da.11601

La intimidad de los ciudadanos en la sala de espera: hacia una directiva europea de protección física de datos personales

The privacy of citizens in the waiting room: Toward a european directive on the physical protection of personal data

Caja Moya, Cristina
Facultad de Ciencias Sociales y Jurídicas. Universidad del Atlántico Medio (España – Spain)
ORCID: https://orcid.org/0000-0003-3878-8721
cristina.caja@pdi.atlanticomedio.es

NOTA BIOGRÁFICA

Jueza y doctora por la Universidad de Las Palmas de Gran Canaria. Docente e investigadora en la Universidad del Atlántico Medio. Ha coorganizado foros internacionales, publicado sobre mediación, uso de IA en Derecho, protección de datos y Derecho Civil, y es delegada del FIMEP en Canarias y miembro de ODR Latinoamérica.

Quiroga Rodríguez, Elio
Facultad de Ciencias Sociales y Jurídicas. Universidad del Atlántico Medio (España – Spain)
ORCID: https://orcid.org/0000-0002-4912-1941
elio.quiroga@pdi.atlanticomedio.es

NOTA BIOGRÁFICA

Ingeniero informático, máster en Astrofísica y doctorando en Ciencias Sociales. Guionista, director, productor y novelista galardonado con premios como el Minotauro y el Policía Nacional. Ha impartido cursos en diversas instituciones y dirigido el Canarias Mediafest. Actualmente es docente e investigador en la Universidad del Atlántico Medio.

RESUMEN

Objetivos: el trabajo busca evidenciar y criticar la desconexión entre el desarrollo de marcos normativos digitales avanzados –como el Plan Estratégico 2025-2030 de la Agencia Española de Protección de Datos (AEPD), enfocado en la inteligencia artificial y la innovación tecnológica– y la persistente vulneración del derecho a la intimidad en los espacios físicos de las Administraciones públicas. Asimismo, pretende impulsar una reflexión sobre la necesidad de extender la protección de datos más allá del entorno digital. **Metodología:** se realiza un análisis crítico y comparativo entre las políticas públicas actuales de protección de datos y las prácticas reales observadas en entornos físicos de atención ciudadana. El estudio examina ejemplos de hospitales, oficinas de empleo y sedes tributarias, contrastando la situación del sector público con los avances del ámbito privado, especialmente el bancario. **Resultados:** el análisis revela una negligencia estructural en la protección de la intimidad dentro de los espacios físicos públicos. Las personas, en contextos de vulnerabilidad, se ven obligadas a ceder su privacidad para acceder a servicios básicos. Se constata una miopía institucional que privilegia la eficiencia burocrática

sobre la dignidad humana, perpetuando un modelo de atención que ignora los principios fundamentales de protección de datos. **Conclusiones:** el estudio propone una hoja de ruta de medidas obligatorias para revertir esta situación: a) Incorporar evaluaciones de impacto sobre privacidad en el diseño de espacios públicos. b) Desarrollar formación especializada para el personal administrativo. c) Implementar garantías arquitectónicas mínimas que aseguren la confidencialidad. Todo ello debe enmarcarse bajo el principio de «privacidad desde el diseño» (privacy by design), con el objetivo de inspirar una futura directiva europea que garantice la efectividad del derecho fundamental a la protección de datos tanto en el ámbito digital como en el físico.

PALABRAS CLAVE

Intimidad en espacios públicos; protección de datos; Administración pública; directiva europea.

ABSTRACT

Objectives: The paper seeks to highlight and critique the disconnection between the development of advanced digital regulatory frameworks –such as the 2025-2030 Strategic Plan of the Spanish Data Protection Agency (AEPD), focused on artificial intelligence and technological innovation– and the persistent violation of the right to privacy in the physical spaces of public administrations. It also aims to encourage reflection on the need to extend data protection beyond the digital environment. **Methodology:** A critical and comparative analysis is conducted between current public data protection policies and the actual practices observed in physical spaces of citizen service. The study examines examples from hospitals, employment offices, and tax agencies, contrasting the public sector's shortcomings with the progress made in the private sector, particularly in banking. **Results:** The analysis reveals structural negligence in the protection of privacy within public physical spaces. Individuals, often in vulnerable situations, are forced to surrender their privacy in order to access basic services. The study identifies an institutional short-sightedness that prioritizes bureaucratic efficiency over human dignity, perpetuating a model of service that disregards fundamental principles of data protection. **Conclusions:** The study proposes a roadmap of mandatory measures to reverse this situation: a) Incorporate privacy impact assessments into the design of public spaces. b) Develop specialized training for administrative personnel. c) Implement minimum architectural safeguards to ensure confidentiality. All these measures should be framed under the principle of «privacy by design» with the aim of inspiring a future European directive that guarantees the effectiveness of the fundamental right to data protection both in the digital and physical spheres.

KEYWORDS

Privacy in public spaces; administrative negligence; applied GDPR; public administration; European directive.

SUMARIO

INTRODUCCIÓN[1]

El debate sobre la protección de datos y la intimidad en la esfera pública suele orbitar, casi en exclusiva, alrededor del mundo digital. Normativas pioneras como el Reglamento General de Protección de Datos (RGPD)[2] y ambiciosos marcos estratégicos, como el recientemente presentado por la AEPD para el periodo 2025-2030[3], centran sus esfuerzos en afrontar los desafíos que plantean la inteligencia artificial, el *big data*, el internet de las cosas y otras tecnologías disruptivas (Antón *et al.,* 2010).

Esta focalización es, sin duda, necesaria y valiosa. Sin embargo, esa mirada al futuro tecnológico ha generado una peligrosa y paradójica zona de sombra: la desatención absoluta a la intimidad en el espacio físico donde los ciudadanos interactúan con sus Administraciones. Mientras se diseñan sofisticados sistemas de supervisión algorítmica y se debaten los neuroderechos, se perpetúa y normaliza una vulneración masiva, sistémica y cotidiana de los derechos fundamentales en hospitales, oficinas de empleo y sedes tributarias.

Hemos aceptado renuncias a derechos de intimidad en los controles aeroportuarios, en los juzgados, en las calles y, en general, en una sociedad –en una suerte de «cultura de la vigilancia» (Lyon, 2018)– que se ha convertido, a causa de unas redes sociales omnipresentes y voraces, en un auténtico comercio de lo íntimo. Precisamente por ello, son las instituciones públicas las que deben comenzar a revertir esta peligrosa tendencia, dando ejemplo de respeto a los derechos fundamentales y proporcionando formación y orientación ciudadana sobre ellos (Zuboff, 2015).

Esta contradicción revela una fractura profunda en la concepción misma del derecho a la protección de datos. Se ha construido un robusto castillo normativo para defender la privacidad en el ciberespacio, mientras se deja abandonada a su suerte en el mundo real, en esos espacios públicos donde la ciudadanía, a menudo en momentos de máxima vulnerabilidad, se ve forzada a sacrificar su intimidad como peaje para acceder a servicios esenciales (Lynskey, 2015). La espera en grupo en urgencias, la obligación de relatar dramas personales en salas abarrotadas del Servicio Público de Empleo Estatal (SEPE) o la exposición oral de datos sensibles en mostradores públicos no son disfunciones menores o anécdotas: son el síntoma de una miopía institucional que prioriza la eficiencia burocrática, la reducción de costes y la gestión de flujos masivos de personas por encima de la dignidad individual. Se trata de una negligencia estructural que normaliza lo inexcusable (Reding, 2011).

Resulta profundamente ilustrativo que sea el sector bancario privado, impulsado por la lógica comercial de la confianza y la experiencia del cliente, y no el sector público –garante último de los derechos fundamentales (Ridaura Martínez, 2021)– el que haya dado los primeros pasos tangibles para mitigar este problema. La instalación de mamparas que separan espacios, aunque acústicamente imperfectas, simboliza un reconocimiento tácito de la necesidad de un mínimo de intimidad para tratar asuntos sensibles (Hijmans, 2016). Esta evolución privada pone en evidencia la parálisis pública y plantea una incómoda pregunta: ¿cómo es posible que la lógica del mercado identifique antes que la del interés general la necesidad de proteger la dignidad en la interacción presencial?

Ante este escenario, resulta imperativo reenfocar el debate y ampliar el alcance de la «innovación responsable» que pregona el plan de la AEPD, para que no se limite al ámbito digital, sino que penetre también en el diseño de los espacios físicos. La defensa de la dignidad en la era digital no puede construirse sobre el debilitamiento de la dignidad en la era física. Este análisis pretende, por tanto, desvelar esta contradicción fundamental, examinar las causas profundas de la negligencia administrativa y, sobre todo, esbozar una hoja de ruta de medidas obligatorias que, partiendo de España, pueda aspirar a convertirse en una directiva europea (Edwards y Veale, 2017). El objetivo es claro: tender un puente entre el marco legal de vanguardia y la experiencia tangible del ciudadano, garantizando que el derecho fundamental a la protección de datos sea una realidad efectiva en todos los ámbitos de la vida, tanto en la pantalla como en la ventanilla.

Cabe plantear si la reivindicación de un trato digno y confidencial en las oficinas públicas dimana directamente del derecho fundamental a la intimidad (art. 18.1 CE) y no requiere de una extensión –acaso forzada– del derecho a la protección de datos personales (art. 18.4 CE), concebido históricamente como un escudo frente a los riesgos del tratamiento automatizado. La distinción doctrinal y jurisprudencial entre ambos

[1] Este artículo no ha contado con financiación pública ni privada.

[2] 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 – RGPD). *Diario Oficial de la Unión Europea*, L 119, pp. 1-88.

[3] Agencia Española de Protección de Datos (2024). Plan Estratégico 2025-2030: Innovación responsable y defensa de la dignidad en la era digital.

derechos, magistralmente sintetizada en la STC 292/2000, es incuestionable: la intimidad opera como un límite a la intromisión indeseada, mientras que la protección de datos confiere un poder de control sobre la información personal (Piñar Mañas, 2014). Sin embargo, es precisamente en la intersección donde este trabajo sitúa su aportación. La vulneración masiva en salas de espera y mostradores no es solo una intromisión en la esfera privada (art. 18.1 CE), sino también, y de forma inherente, un tratamiento de datos personales en su definición más amplia y literal del RGPD: toda información sobre una persona física identificada o identificable. La verbalización de una enfermedad, la exposición de un documento con datos económicos o la visualización de un estado de salud en una pantalla constituyen actos de tratamiento –comunicación y divulgación– que acontecen en un soporte físico (el sonido, la imagen) y en un contexto organizativo. El derecho a la protección de datos (Carazo Liébana, 2023), con su arsenal de principios proactivos (tales como privacidad desde el diseño, evaluación de impacto o rendición de cuentas), no se limita al riesgo de la difusión digital ilimitada; se proyecta sobre cualquier tratamiento que pueda menoscabar la dignidad y la autodeterminación informativa. Argumentar que su aplicación se circunscribe al ámbito automatizado supone restringir artificialmente su potencial garantista. La propuesta aquí defendida no diluye la especificidad de cada derecho, sino que reconoce que, en la práctica administrativa contemporánea, la lesión de la intimidad se produce frecuentemente a través de un tratamiento negligente de datos en el espacio físico. Por tanto, el marco de la protección de datos –más desarrollado, concreto y dotado de mecanismos de ejecución– se erige en la herramienta jurídica más idónea para operativizar y garantizar ese «poder de disposición» sobre la información personal que la STC 292/2000 enuncia, incluso cuando la amenaza no proviene de una base de datos, sino de una sala mal diseñada o de un procedimiento presencial que fuerza la divulgación. Lejos de ser una extensión forzada, esta lectura integral es la consecuencia lógica de un concepto de «dato personal» neutro respecto al soporte y de una comprensión del «tratamiento» que abarca toda operación realizada sobre información identificativa, sea esta digital, oral o visual.

1. METODOLOGÍA

El presente estudio adopta una metodología jurídico-analítica y exploratoria, centrada en la identificación de un vacío normativo y operativo en la aplicación del derecho fundamental a la intimidad en los espacios físicos de atención pública. El trabajo se apoya en tres ejes complementarios: análisis normativo-doctrinal, observación empírica indirecta y propuesta proactiva de diseño institucional.

En primer lugar, se realiza un examen sistemático del marco jurídico vigente en materia de protección de datos –principalmente el Reglamento (UE) 2016/679 (RGPD), la Ley Orgánica 3/2018 (LOPDGDD)[4] y el Plan Estratégico 2025-2030 de la AEPD–, contrastándolo con la doctrina europea y comparada sobre el principio de *privacy by design and by default* (Cavoukian, 2009; Clarke, 2009; Burdon y McKillop, 2013). Este análisis se orienta a detectar la ausencia de traslación material de dichos principios al entorno físico y arquitectónico de la Administración pública.

En segundo lugar, se incorpora una observación empírica indirecta de las prácticas administrativas cotidianas –hospitales, oficinas de empleo, sedes tributarias y juzgados– recogidas mediante revisión de informes públicos, resoluciones de la AEPD y experiencias de campo documentadas en estudios sectoriales. Esta aproximación permite identificar patrones recurrentes de exposición indebida de información personal y deficiencias estructurales de privacidad presencial, lo que justifica el diagnóstico de «negligencia institucional sistemática».

Finalmente, se utiliza un enfoque propositivo-normativo, propio del derecho comparado y de la política regulatoria, para formular una hoja de ruta estructurada en seis pilares que traduce los principios del RGPD al plano físico y organizativo. Este enfoque combina el análisis jurídico con herramientas de evaluación de impacto, ética pública y diseño institucional, proponiendo estándares verificables que puedan ser elevados a rango normativo, primero en el ámbito nacional y, posteriormente, en el europeo.

La combinación de estos tres niveles –normativo, empírico y propositivo– permite ofrecer una visión holística y aplicada de la protección de datos en el entorno presencial, superando la habitual fragmentación entre el discurso jurídico-tecnológico y la realidad cotidiana del ciudadano.

[4] 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).

Cabe indicar, y los autores asumen estas decisiones, que la selección de casos puede indicar un cierto *cherry-picking*, al no basarse en una sistemática, sino en unos ejemplos elegidos que pueden resultar elegidos *ad hoc* para la discusión. Esta limitación del trabajo se asume en tanto llamada de atención sobre un estado de cosas, indicándose que un posible paso subsiguiente sería un estudio sistemático de casos.

2. MARCO NORMATIVO EUROPEO APLICABLE A LA PROTECCIÓN JURÍDICA DE LA INTIMIDAD

El marco jurídico europeo de protección de datos personales ofrece una base sólida para extender el derecho a la intimidad más allá del entorno digital, aunque aún carece de una regulación específica sobre la privacidad en los espacios físicos de atención pública. La normativa vigente, encabezada por el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 (RGPD), configura un sistema de garantías que, interpretado de forma sistemática y teleológica, abarca también las dimensiones materiales y organizativas del tratamiento de la información.

El art. 25 RGPD, que consagra el principio de *privacy by design and by default*, impone a los responsables y encargados del tratamiento la obligación de adoptar «medidas técnicas y organizativas apropiadas» para garantizar la efectividad de los derechos fundamentales, atendiendo al contexto, alcance y fines del tratamiento. Aunque la práctica lo ha circunscrito al desarrollo de *software* o plataformas digitales, su alcance es más amplio: la referencia a las «medidas organizativas» comprende igualmente la arquitectura institucional y espacial en que se realiza el tratamiento. Por tanto, las Administraciones públicas deberían configurar físicamente sus espacios y procedimientos de atención de modo que preserven la confidencialidad y eviten la exposición innecesaria de datos personales en lugares como hospitales, oficinas de empleo o juzgados.

El art. 32 RGPD, relativo a la seguridad del tratamiento, refuerza esta obligación al requerir medidas que garanticen la «confidencialidad, integridad y disponibilidad» de los datos personales. Si bien la doctrina y la práctica administrativa han centrado esta exigencia en los sistemas informáticos, la seguridad y la confidencialidad son también categorías espaciales y relacionales: una conversación sobre la salud o la situación económica o familiar del ciudadano constituye un tratamiento de datos personales que exige el mismo nivel de protección, cualquiera que sea el soporte o el entorno en que se produzca (De Hert y Papakonstantinou, 2016; González Fuster, 2014).

La Carta de los Derechos Fundamentales de la Unión Europea (2000)[5] refuerza esta lectura integral. Sus arts. 7 y 8 reconocen, respectivamente, el derecho al respeto de la vida privada y familiar y el derecho a la protección de los datos personales, con un alcance que abarca tanto las interacciones digitales como las presenciales. El Tribunal de Justicia de la Unión Europea ha reiterado que estos derechos se aplican a cualquier tratamiento que implique revelación o comunicación de información personal, sin limitarse a los entornos informáticos (SSTJUE C-468/10 y C-469/10, ASNEF y FECEMD; C-582/14, Breyer)[6]. En consecuencia, las condiciones materiales en que los ciudadanos son atendidos en dependencias públicas forman parte del ámbito de protección de estos derechos fundamentales (Puerta Domínguez, 2023).

A esta concepción expansiva se suma el Convenio 108+ del Consejo de Europa[7], modernizado en 2018, sobre la protección de las personas respecto al tratamiento automatizado de datos personales. Su art. 7 obliga a los Estados parte a adoptar medidas «técnicas y organizativas adecuadas» para salvaguardar la confidencialidad y seguridad de los datos, lo que –según su exposición de motivos– incluye todos los contextos en que se maneje información personal, con independencia del soporte o la tecnología utilizada. Este tratado, ratificado por España, es el primer instrumento internacional que reconoce expresamente la dimensión ética y ambiental de la privacidad, abriendo la puerta a una interpretación material del derecho a la intimidad que comprenda el entorno físico y social en que se ejerce.

---

[5] Carta de los Derechos Fundamentales de la Unión Europea, proclamada en Niza el 7 de diciembre de 2000 (DOUE C 364, de 18 de diciembre de 2000, pp. 1-22), incorporada con valor jurídico vinculante por el Tratado de Lisboa (art. 6 TUE).

[6] Tribunal de Justicia de la Unión Europea (TJUE) (2011, 24 de noviembre). Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) y Federación de Comercio Electrónico y Marketing Directo (FECEMD), asuntos acumulados C-468/10 y C-469/10. ECLI:EU:C:2011:777.TJUE. (2016, 19 de octubre). Patrick Breyer / Bundesrepublik Deutschland, asunto C-582/14. ECLI:EU:C:2016:779.

[7] Convenio 108+ del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, hecho en Estrasburgo el 10 de octubre de 2018 (Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, modificado por el Protocolo CETS núm. 223). Ratificado por España mediante Instrumento de 9 de junio de 2023 (BOE núm. 194, de 14 de agosto de 2023).

Asimismo, la Directiva (UE) 2016/680, relativa a la protección de datos en el ámbito penal y judicial[8], establece en su art. 20 la obligación de garantizar la confidencialidad y seguridad del tratamiento «en todas las fases del procedimiento» (Rodríguez Roca, 2022). La doctrina (Hijmans, 2016; Kosta, 2013) ha subrayado que estas garantías no se limitan al tratamiento informático, sino que alcanzan también las dimensiones organizativas y materiales en que se gestionan los datos personales, lo que puede incluir la configuración física de juzgados, dependencias policiales y servicios auxiliares de justicia. Aunque su ámbito se circunscribe a las autoridades competentes en materia penal, constituye una referencia interpretativa valiosa para diseñar garantías análogas en otros espacios institucionales donde se traten datos sensibles.

El Comité Europeo de Protección de Datos (CEPD) ha reforzado esta visión holística en sus Directrices 4/2019[9] sobre el art. 25 RGPD, al subrayar que la protección de datos desde el diseño debe ser «contextual, transversal y proactiva», alcanzando tanto las infraestructuras digitales como las físicas donde se desarrollan los tratamientos. El CEPD insta a las autoridades nacionales a incorporar la privacidad en el diseño de los servicios públicos presenciales, reconociendo que la exposición acústica o visual de información personal puede vulnerar el principio de confidencialidad del art. 5.1.f RGPD.

Por su parte, la Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), en su art. 28.2, impone a las Administraciones públicas la obligación de adoptar medidas organizativas que garanticen la confidencialidad de los datos personales tratados. Aunque no detalla las medidas concretas, esta obligación se extiende a las condiciones materiales y ambientales del trato con la ciudadanía. La Agencia Española de Protección de Datos (AEPD) ha dictado resoluciones en las que advierte que prácticas como anunciar en voz alta nombres o verificar datos personales en mostradores abiertos vulneran el principio de confidencialidad del art. 5.1.f RGPD.

En conjunto, este entramado normativo europeo y nacional demuestra que, aunque aún no exista una directiva específica sobre la protección de la intimidad en espacios físicos de atención pública, sí existe una base jurídica suficiente para su desarrollo. La futura Directiva Europea de Protección Física de Datos Personales no sería una innovación exógena, sino la materialización coherente del espíritu del RGPD, de la Carta de Derechos Fundamentales y del Convenio 108+, completando así la transición de una privacidad concebida como principio digital a una privacidad plenamente humana e integral.

En coherencia con la orientación del legislador europeo hacia un ecosistema de gobernanza responsable de los datos –reflejada en el Reglamento (UE) 2022/868 (Data Governance Act)[10] y en el Reglamento (UE) 2024/1689 (Artificial Intelligence Act)–, el principio de *privacy by design* debe proyectarse también sobre los entornos físicos de interacción administrativa, garantizando que la innovación tecnológica no se desarrolle a costa de la dignidad del ciudadano.

3. RESULTADOS: ANÁLISIS CRÍTICO DE RESOLUCIONES DE LA AEPD COMO ILUSTRACIÓN DE LA NEGLIGENCIA EN LA PROTECCIÓN FÍSICA DE LA INTIMIDAD

A continuación, se sintetizan resoluciones y documentos de la AEPD que ilustran la proyección del RGPD sobre el espacio físico de atención al público –en especial, salas de espera, mostradores abiertos y sistemas de turno/llamada–, y que respaldan la necesidad de medidas organizativas y arquitectónicas para garantizar la confidencialidad (art. 5.1.f y 32 RGPD).

3.1. Exposición acústica y visual: la intimidad negada en la interacción directa

Los casos más reveladores son aquellos en los que la intimidad se ve comprometida por la simple arquitectura del espacio y el diseño de los procedimientos. La Resolución E-04967-2020, sobre un sistema de citas que enumeraba nombres en voz alta, es ejemplar. Aunque el caso se archivó tras la corrección técnica, la propia

[8] Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos, y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo (DOUE L 119, de 4 de mayo de 2016, pp. 89-131).

[9] Comité Europeo de Protección de Datos (CEPD) (2020). *Directrices 4/2019 sobre el artículo 25 del Reglamento (*UE*) 2016/679: Protección de datos desde el diseño y por defecto.* Aprobadas el 13 de noviembre de 2019 y adoptadas definitivamente el 20 de octubre de 2020.

[10] Reglamento (UE) 2022/868 del Parlamento Europeo y del Consejo, de 30 de mayo de 2022, relativo a la gobernanza de los datos y por el que se modifica el Reglamento (UE) 2018/1724 (Reglamento de Gobernanza de Datos o Data Governance Act) (DOUE L 152, de 3 de junio de 2022, pp. 1-44).

intervención de la AEPD deja claro que la identificación auditiva de personas en un espacio compartido constituye un tratamiento de datos que exige garantías de confidencialidad (art. 5.1.f RGPD). Este no es un problema menor o técnico: es la materialización de un diseño hostil a la privacidad, donde la eficiencia operativa (llamar a los pacientes) se prioriza sobre su derecho a no revelar su identidad ante desconocidos. De manera análoga, la Resolución PS/00317/2022, concerniente a la visualización pública de la temperatura corporal en una clínica, subraya que la confidencialidad tiene una dimensión física ineludible. La exposición visual de un dato de salud en una sala de espera vulnera el mismo principio de confidencialidad que protege una base de datos digital. Ambos casos ilustran una miopía organizativa que ignora que el tratamiento de datos personales comienza en el momento en que se verbaliza o se hace visible en un espacio físico, no cuando se registra en un sistema informático.

3.2. Confidencialidad sistémica: más allá del dato digital

La Resolución PS-00250-2021, por su parte, aborda accesos indebidos a historias clínicas, un fallo tradicionalmente asociado a la seguridad digital. Sin embargo, su mención es relevante porque la AEPD amonestó al servicio de salud por deficiencias tanto técnicas como organizativas. Esto refuerza la tesis de que la confidencialidad es un principio integral: la falta de medidas organizativas adecuadas (que incluyen la formación del personal y los protocolos de acceso físico a las áreas de consulta) crea un entorno donde la violación de la intimidad es estructural, independientemente de la fortaleza de los *firewalls* digitales. La seguridad del dato comienza en el espacio donde se habla de él.

En síntesis, el examen conjunto de estas resoluciones no busca presentar un cuadro estandarizado, sino realizar un diagnóstico profundo: la AEPD, en el ejercicio de sus funciones, ya está identificando y sancionando vulneraciones de la intimidad que ocurren físicamente (por exposición acústica, visual o vigilancia corporal). La desconexión radica en que estas actuaciones son reactivas (surgen de reclamaciones) y no han generado aún un marco preventivo y obligatorio de «privacidad desde el diseño» aplicado a los espacios. Estos casos son, por tanto, la prueba empírica de la negligencia estructural y la base jurídica sobre la que debe construirse la reforma propuesta.

3.3. Confidencialidad y seguridad en entorno sanitario (PS-00250-2021, Servicio Extremeño de Salud)[11]

- Hechos. Accesos indebidos a historia clínica; déficit de medidas técnicas y organizativas (González Suárez, 2025).
- Criterio AEPD. Apercibimiento por arts. 32 y 5.1.f RGPD; exige reforzar confidencialidad.
- Relevancia. Aun sin referirse a «mostradores», evidencia que la confidencialidad en sanidad es también espacial y organizativa: lo que se dice o se expone en el punto de atención está amparado por los mismos principios (Memoria AEPD 2021 y «Salud – principales reclamaciones»).

3.4. Visualización pública de datos (temperatura) en clínica (Resolución: PS/00317/2022 – Centro Médico Salus Baleares, S. L.)[12]

- Hechos: el dispositivo de control de temperatura permitía que pacientes y personal en sala de espera viesen la temperatura tomada a otros pacientes.
- Criterio AEPD: vulneración de confidencialidad (art. 5.1.f RGPD) y seguridad (art. 32 RGPD); la exposición visual de información personal en espacio común es contraria al RGPD.
- Relevancia: ilustra que la confidencialidad tiene dimensión física (lo que se ve/oye en la sala) y no solo digital. Refuerza tus pilares sobre diseño de salas, paneles y flujos.

4. DISCUSIÓN

La promulgación del RGPD ha representado un hito decisivo en la defensa de los derechos digitales de los ciudadanos europeos, al establecer un marco jurídico robusto y ambicioso para la era digital (De Hert y

[11] AEPD (2021). Resolución PS-00250-2021 (1 de julio de 2021).

[12] AEPD (2022). Resolución PS-00317-2022. https://www.aepd.es/documento/ps-00317-2022.pdf

Papakonstantinou, 2016; González Fuster, 2014). El *Plan Estratégico 2025-2030 de la AEPD, Innovación responsable y defensa de la dignidad en la era digital*[13], constituye una manifestación clara de este compromiso, al orientarse hacia la supervisión de tecnologías disruptivas como la inteligencia artificial, la promoción de una cultura de cumplimiento y la consolidación de una agencia inteligente y proactiva.

Sin embargo, persiste una peligrosa desconexión entre este sofisticado marco normativo y tecnológico y la realidad tangible que experimentan millones de ciudadanos en sus interacciones cotidianas con las Administraciones públicas (Pedraza Córdoba, 2023). Mientras la AEPD diseña sistemas de inteligencia artificial para la supervisión automatizada y promueve debates sobre neuroderechos o *blockchain*, en la planta física de un hospital, en la sala de espera de una oficina de empleo o en la ventanilla de Hacienda se produce un progresivo debilitamiento del derecho fundamental a la protección de datos y a la intimidad, invisible para la propia arquitectura legal creada para salvaguardarlo (Arenas Ramiro, 2023).

Este olvido estructural no constituye una mera anécdota ni una disfunción menor, sino el síntoma de una miopía institucional profunda, que antepone la eficiencia administrativa, la reducción de costes a corto plazo y la gestión de flujos masivos de personas a la dignidad individual. La ciudadanía se ve forzada a renunciar a su intimidad como peaje obligatorio para acceder a servicios públicos esenciales: la salud, las prestaciones por desempleo o la justicia (Nissenbaum, 2009; Solove, 2006).

La espera colectiva en urgencias hospitalarias, donde pacientes con patologías diversas y potencialmente estigmatizantes deben compartir un espacio angosto, supone una violación de la intimidad más básica. El requisito de relatar problemas personales, financieros o familiares de extrema sensibilidad en salas abiertas del SEPE, rodeado de desconocidos, convierte una situación ya vulnerable en una experiencia humillante. Y la práctica –todavía habitual en muchas oficinas de la Agencia Tributaria– de solicitar o confirmar en voz alta datos personales, financieros o familiares ante otras personas expone la vida privada del individuo al escrutinio involuntario de quienes esperan su turno.

La imposibilidad estructural de ser atendido en un espacio confidencial, a pesar de que la ley ampara ese derecho, demuestra que la protección de datos se concibe con frecuencia como un principio abstracto aplicable solo al entorno digital, y no como un derecho fundamental de aplicación transversal que debe impregnar todas las capas de la relación entre el Estado y el ciudadano (Flores Cabrera, 2023).

Resulta paradigmático –y casi irónico– que sea el sector bancario privado, sujeto al mismo RGPD y a la supervisión de la AEPD, el que, guiado por la lógica comercial de la confianza y la experiencia del cliente, haya dado los primeros pasos tangibles para mitigar este problema. La instalación de mamparas que separan los espacios de atención, aunque insuficientes desde un punto de vista acústico, representa un reconocimiento tácito de la necesidad de un mínimo de intimidad para tratar asuntos sensibles.

Esta evolución, impulsada por el mercado, pone de relieve una paradoja preocupante: las instituciones privadas, movidas por la búsqueda de rentabilidad y reputación, han comenzado a comprender la privacidad como un valor añadido, mientras que las instituciones públicas, garantes últimas del interés general y de los derechos fundamentales, permanecen rezagadas en la materialización física de esos mismos derechos (Bellanova y González Fuster, 2013).

Con todo, sería incompleto ignorar los progresos realizados en la mejora del trato al ciudadano, entendido también como usuario del servicio público. En numerosos ámbitos se han implantado sistemas de identificación en salas de espera que evitan la mención expresa del nombre completo, recurriendo a iniciales o a códigos numéricos. Del mismo modo, en el entorno hospitalario –especialmente en los servicios de urgencias– se han reforzado de manera significativa los controles de acceso y la gestión de acompañantes, tratándose estos espacios como áreas de acceso restringido. La comunicación de información clínica, además, queda supeditada a la debida acreditación de la identidad y del vínculo con el paciente, lo que evidencia una mayor sensibilidad institucional hacia la protección de la intimidad personal.

4.1. Causas estructurales de la negligencia administrativa

La negligencia de las Administraciones públicas en materia de intimidad no es casual, sino que responde a una combinación de factores estructurales y culturales que se retroalimentan.

En primer lugar, persiste una cultura administrativa heredada del siglo XX –y, en parte, del XIX– en la que el ciudadano era concebido como un sujeto pasivo, un número de expediente y no un titular activo de

[13] AEPD (2024). Plan Estratégico 2025-2030: Innovación responsable y defensa de la dignidad en la era digital.

derechos (Altman, 1977). La lógica burocrática tradicional priorizaba –y en muchos casos aún prioriza– la uniformidad, el control y la tramitación masiva de expedientes por encima de la personalización y el respeto a la individualidad. La intimidad se sacrificaba así en el altar de la eficiencia procedimental, un intercambio que el marco constitucional y el RGPD ya no permiten, pero cuya inercia institucional sigue siendo poderosa (Kosta, 2013).

En segundo lugar, se evidencia un problema crónico de infraestructura y financiación. Buena parte del parque edificatorio público fue diseñado en una época en la que la privacidad ciudadana no constituía un criterio arquitectónico ni organizativo. Reformar esos espacios supone un coste elevado que compite con otras prioridades presupuestarias –como la contratación de personal o la modernización digital–, lo que perpetúa la brecha entre la infraestructura física y la ambición digital que promueve la AEPD en su Plan Estratégico.

En tercer lugar, se aprecia una aplicación fragmentaria del principio de «protección desde el diseño y por defecto» (privacy by design and by default), uno de los pilares del RGPD y reiteradamente invocado por la AEPD (Cavoukian, 2009). Dicho principio se aplica casi exclusivamente al desarrollo de *software*, plataformas digitales y procesos técnicos, pero rara vez se extiende al diseño espacial u organizativo. ¿De qué sirve una base de datos perfectamente cifrada si el dato más sensible se pronuncia en voz alta en una sala pública? El resultado es un entorno administrativo que continúa siendo, en gran medida, «hostil a la privacidad» por defecto.

Finalmente, existe una ausencia notoria de directrices y normas vinculantes, tanto a nivel europeo como nacional, que trasladen los principios generales del RGPD al diseño físico de los espacios públicos y a los procedimientos de atención presencial. El RGPD establece el qué –la obligación de proteger los datos personales–, pero no el cómo debe materializarse esa protección en la interacción directa con el ciudadano. Esta falta de concreción facilita interpretaciones laxas e implementaciones deficientes, y deja a las Administraciones sin un mandato operativo claro ni mecanismos específicos de supervisión por parte de las autoridades de control.

4.2. Consecuencias prácticas sobre la intimidad ciudadana

Las deficiencias estructurales en materia de intimidad no solo tienen un impacto operativo en la atención al público, sino que transforman la relación entre la Administración y la ciudadanía. Su efecto más profundo es la pérdida de la expectativa legítima de confidencialidad, entendida no como un privilegio, sino como un presupuesto del ejercicio de los derechos fundamentales.

En primer lugar, la falta de mecanismos institucionales que garanticen la privacidad física genera una asimetría relacional entre la Administración –que controla el espacio, los tiempos y las condiciones de atención– y el ciudadano, que se ve compelido a exponer datos personales en entornos donde la intimidad se vuelve imposible. Esa exposición forzada vulnera el principio de autodeterminación informativa y reduce la protección de datos a una formalidad documental, desvinculada de la experiencia real del administrado.

En segundo lugar, la reiteración de estas prácticas produce un efecto de habituación: el ciudadano interioriza que la revelación pública de su vida personal es el precio inevitable para acceder a un servicio público. Este fenómeno, que puede describirse como una «normalización institucional del condicionamiento de la intimidad», o de una «intimidad condicionada a eficiencia», podría erosionar el contenido esencial del art. 18 CE y contradice el mandato del art. 103 CE, que exige que la Administración actúe al servicio objetivo del interés general y con pleno respeto a la dignidad de la persona.

En tercer lugar, la falta de espacios y protocolos confidenciales genera desconfianza y retraimiento. Cuando el ciudadano percibe que su entorno de atención no es seguro, tiende a omitir información o a posponer trámites, lo que dificulta la eficacia administrativa y la protección de otros derechos sustantivos (como la salud, la asistencia social o la justicia). La privacidad, por tanto, no es un lujo ni un complemento estético del servicio público, sino una condición de posibilidad de la Administración garantista.

Finalmente, la consecuencia más grave es simbólica: la deslegitimación del propio discurso institucional sobre la protección de datos. Mientras las Administraciones invierten recursos en digitalizar garantías normativas, la persistencia de espacios físicos hostiles a la intimidad vacía de coherencia su compromiso ético y jurídico. El resultado es una brecha entre el lenguaje de la protección y la práctica del desamparo, que debilita la confianza democrática y desvirtúa la idea misma de «innovación responsable» proclamada por la AEPD.

4.3. Propuesta de reforma y alineación con el Plan Estratégico de la AEPD

El Plan Estratégico de la AEPD 2025-2030, con su énfasis en la proactividad, la prevención, la defensa de los colectivos vulnerables y la promoción de una cultura de cumplimiento, ofrece el marco perfecto para abordar esta desconexión. No se trata de crear una normativa paralela, sino de interpretar y aplicar el espíritu y la letra del RGPD y de la Ley Orgánica de Protección de Datos en el ámbito físico con el mismo rigor que se aplica en el digital. La «visión» del Plan de consolidar a la AEPD como una autoridad líder que «orienta y encauza adecuadamente los desarrollos tecnológicos» debe extenderse también a orientar y encauzar el desarrollo de los espacios públicos de atención.

Para ello, es imperativo desarrollar un conjunto de medidas concretas, prácticas y auditables que puedan ser adoptadas primero como estándar nacional en España y, posteriormente, dada la naturaleza transversal del problema, propulsadas como una directiva comunitaria de la Unión Europea. Esta directiva debería tener como objetivo armonizar la protección de la intimidad en la atención presencial en todos los Estados miembros, estableciendo unos mínimos comunes que garanticen que el derecho fundamental a la protección de datos es efectivo en todas las dimensiones de la vida ciudadana. La AEPD, en línea con su principio rector de «Internacionalización e influencia» y su Eje 5 de «Liderazgo e influencia estratégica internacional», debería ser la impulsora de esta iniciativa a nivel del Comité Europeo de Protección de Datos (CEPD).

Las medidas obligatorias deberían articularse alrededor de varios pilares fundamentales.

4.3.1. *Primer pilar: evaluación obligatoria de impacto en la intimidad y protección de datos en el diseño de espacios y procedimientos presenciales*

El primero de los pilares sería la Evaluación Obligatoria de Impacto en la Intimidad y Protección de Datos en el Diseño de Espacios y Procedimientos Presenciales. Así como se exige una Evaluación de Impacto para tratamientos de datos de alto riesgo (Clarke, 2009), toda reforma, construcción nueva o rediseño de un procedimiento de atención al público que implique la recogida o gestión de datos personales debería incluir una evaluación específica que analice los riesgos para la intimidad en el espacio físico.

Esta evaluación examinaría los flujos de personas, los puntos de fricción donde se intercambia información sensible, la acústica de las salas, la disposición de los mostradores y la existencia de alternativas confidenciales.

El Plan de la AEPD, en su Eje 1 sobre «Una agencia inteligente», promueve el «análisis proactivo sobre sectores» y la «detección temprana de riesgos»; esta medida sería la materialización práctica de ese principio en el entorno físico (Burdon y McKillop, 2013).

4.3.2. *Segundo pilar: implementación de garantías arquitectónicas y de diseño mínimas*

Toda área de atención al público en la que se traten datos de categoría especial –como los relativos a salud, ideología, orientación sexual, creencias religiosas o información financiera, laboral o personal de alto impacto– deberá contar, por defecto**,** con espacios que garanticen la confidencialidad efectiva de la comunicación entre el ciudadano y el personal que le atiende.

Ello implica la existencia obligatoria de cabinas o despachos insonorizados o, al menos, acústicamente aislados**,** destinados a entrevistas personales. Las salas de espera deberán diseñarse de modo que eviten la proximidad forzada y la escucha involuntaria, mediante una distribución inteligente del mobiliario, paneles divisorios y señalética que oriente al usuario hacia zonas de privacidad.

De forma complementaria, los sistemas de aviso y turno deberán incorporar un dispositivo de solicitud de atención en condiciones reforzadas de confidencialidad (que podríamos llamar coloquialmente un «botón de atención confidencial») o una suerte de mecanismo equivalente que permita al ciudadano solicitar un trato más íntimo o reservado sin necesidad de justificarlo. Las pantallas informativas sustituirán la identificación nominal por sistemas de numeración o códigos, evitando así la exposición innecesaria de datos personales.

Los mostradores de atención general deberán diseñarse con criterios de privacidad acústica y visual, utilizando mamparas de cristal con sonido direccional, micrófonos y auriculares que impidan la audición por terceros.

La inversión en esta infraestructura no debe considerarse un gasto**,** sino una exigencia derivada directamente del art. 18 de la Constitución española, del art. 32 del RGPD y de la Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD)**.** Su función es equiparable,

en términos de obligatoriedad y tutela de derechos fundamentales, a las medidas de accesibilidad física para personas con discapacidad o movilidad reducida.

4.3.3. *Tercer pilar: formación obligatoria y especializada del personal de atención al público*

El tercer pilar constituye, con frecuencia, el más decisivo y a la vez el más desatendido: la formación obligatoria, continua y especializada del personal de atención directa al ciudadano. Los funcionarios y trabajadores contratados que desempeñan sus funciones en ventanilla, mostrador o atención telefónica representan la primera línea de defensa del derecho a la intimidad y a la protección de datos personales.

Esta formación no puede limitarse a una exposición genérica de la normativa vigente, sino que debe incluir protocolos prácticos y verificables de actuación:

- Cuándo y cómo derivar al ciudadano a un espacio de atención privada.
- Cómo modular la voz y mantener la distancia prudencial en conversaciones sensibles.
- Cómo sustituir la solicitud oral de datos por el uso de formularios escritos, pantallas táctiles o sistemas digitales seguros.
- Cómo empoderar al ciudadano para que ejerza su derecho a la confidencialidad sin temor a represalias o demoras.

La Agencia Española de Protección de Datos (AEPD), en cumplimiento de su Eje 3 («Promover y acompañar el cumplimiento normativo») y Eje 6 («Una Administración eficaz») del Plan Estratégico de la AEPD 2023-2026, debe incorporar de forma expresa programas de formación y concienciación masiva dirigidos al personal de atención al público, en coordinación con el Instituto Nacional de Administración Pública (INAP) y los órganos competentes de las comunidades autónomas.

Esta capacitación ha de considerarse una obligación institucional derivada del principio de responsabilidad proactiva del art. 5.2 del Reglamento (UE) 2016/679 (RGPD) y del art. 28 de la Ley Orgánica 3/2018 (LOPDGDD), que impone a las Administraciones públicas el deber de garantizar no solo la licitud del tratamiento de datos, sino también la formación adecuada del personal autorizado para dicho tratamiento.

En consecuencia, la formación en privacidad y trato confidencial debe integrarse en los planes de carrera y evaluación de desempeño de todo el personal de atención al público, y su incumplimiento ha de ser considerado un déficit organizativo susceptible de responsabilidad disciplinaria o administrativa, en la medida en que afecta directamente al ejercicio de los derechos fundamentales reconocidos en los arts. 18.1 y 18.4 de la Constitución española[14].

4.3.4. *Cuarto pilar: establecimiento de canales alternativos preferentes y accesibles para minimizar la exposición física*

Este pilar se centra en la creación de canales de comunicación y tramitación que, por su propia arquitectura, prevengan o reduzcan la necesidad de exponer datos personales en espacios físicos compartidos. Se trata de aplicar el principio de «privacidad por diseño y por defecto» (art. 25 RGPD) para ofrecer al ciudadano vías que, de origen, protejan su intimidad. La promoción activa de la cita previa telemática y la tramitación electrónica segura no tiene como único objetivo la eficiencia digital, sino fundamentalmente evitar las aglomeraciones y las esperas en salas comunes donde la confidencialidad se vuelve imposible. Del mismo modo, una atención telefónica bien diseñada, con protocolos robustos de verificación de identidad, puede resolver muchas gestiones sin obligar al ciudadano a desplazarse y revelar información sensible en un mostrador público. Estos canales son, por tanto, herramientas de protección física de la intimidad, al reducir drásticamente los momentos de fricción y exposición personal en el entorno físico administrativo. Su implementación debe ser preferente, complementada siempre con una atención presencial que, cuando sea inevitable, cumpla con los estándares de confidencialidad arquitectónica y procedimental detallados en los demás pilares. Esta aproximación conecta con el objetivo de la AEPD de «facilitar el cumplimiento normativo» y subraya que la protección de datos es un derecho transversal, cuya efectividad depende de un ecosistema de opciones donde la interacción física sea la más segura y digna posible, no la única disponible.

[14] Constitución española, arts. 18.1 y 18.4 (BOE núm. 311, de 29 de diciembre de 1978). El primero reconoce el derecho al honor, a la intimidad personal y familiar y a la propia imagen; el segundo garantiza la limitación del uso de la informática para asegurar el respeto de dichos derechos y de la libertad personal.

4.3.5. *Quinto pilar: protocolos claros para situaciones de vulnerabilidad acentuada*

El quinto pilar implicaría la creación de protocolos claros para situaciones de vulnerabilidad acentuada. Las Administraciones deben disponer de procedimientos específicos y activables de forma inmediata para garantizar una atención confidencial, empática y prioritaria a las personas que, por su situación, son especialmente vulnerables a una violación de su intimidad o dignidad.

Entre estos colectivos se incluyen, a título ejemplificativo, las víctimas de violencia de género, los pacientes oncológicos o con enfermedades infecciosas estigmatizadas, las personas inmersas en procesos de despido colectivo, ERTE o desempleo de larga duración, así como los migrantes en situación administrativa irregular o las personas con discapacidad psicosocial o cognitiva.

Estos protocolos deben contemplar circuitos rápidos de atención reservada, la designación de personal especialmente formado y la posibilidad de activar espacios de atención privada de manera inmediata, sin necesidad de que la persona justifique su solicitud de confidencialidad.

El principio rector de la AEPD de «Defensa del interés general», junto con su enfoque transversal en la protección de colectivos vulnerables, debe tener una traducción operativa concreta en la organización física y funcional de las oficinas públicas, de modo que la protección de datos y la intimidad no dependan del azar, la buena voluntad o la discrecionalidad del empleado, sino de estructuras y procedimientos predefinidos (AEPD, Plan Estratégico 2023-2026).

4.3.6. *Sexto pilar: sistema específico de supervisión, quejas y sanciones*

Por último, deviene esencial la existencia de un sistema específico de supervisión, quejas y sanciones, que garantice la efectividad real de las medidas anteriores. Las autoridades de protección de datos, tanto a nivel nacional como autonómico, deben incorporar en sus planes de inspección y supervisión la evaluación del cumplimiento de las garantías arquitectónicas, procedimentales y formativas adoptadas por las Administraciones públicas en materia de intimidad y confidencialidad presencial.

Debe existir un canal accesible, visible y sencillo para que los ciudadanos reporten vulneraciones de su intimidad en entornos de atención al público, con mecanismos ágiles de tramitación y respuesta.

Estas quejas deben ser investigadas y, en su caso, sancionadas conforme al marco previsto en el Reglamento (UE) 2016/679 (RGPD) y en la Ley Orgánica 3/2018 (LOPDGDD).

El régimen sancionador del RGPD, aplicable también a las Administraciones públicas en casos de incumplimientos graves o sistemáticos, debe extenderse expresamente a las violaciones del deber de confidencialidad presencial, del mismo modo que se aplica ya en ámbitos como la seguridad de la información o la conservación indebida de datos.

El Eje 1 del Plan Estratégico de la AEPD 2023-2026, que promueve una «supervisión más inteligente» y la realización de «auditorías preventivas», debe incorporar este nuevo vector de análisis, orientado a verificar el grado de cumplimiento de las garantías estructurales de intimidad en oficinas y dependencias públicas, asegurando así una protección integral y verificable de la privacidad en el trato directo con la ciudadanía.

La implementación de estas medidas, primero en España y luego como directiva europea, requeriría un esfuerzo coordinado y una fuerte inversión inicial. Sin embargo, el coste de no actuar es infinitamente mayor: es el coste de la desconfianza ciudadana en las instituciones, de la humillación sistemática de los más vulnerables y de la devaluación práctica de un derecho fundamental que queda reducido a un principio teórico. El Plan Estratégico 2025-2030 de la AEPD tiene la ambición de mirar hacia el futuro de la tecnología. Pero el primer paso para construir un futuro digital digno es asegurar que el presente físico en el que vivimos ya respeta esa misma dignidad. La verdadera innovación responsable comienza por garantizar que nadie tenga que renunciar a su intimidad para ser curado, atendido o escuchado por su propia Administración. Convertir esta visión en una realidad tangible sería el legado más profundo y humano que este plan podría dejar no solo para España, sino para toda Europa.

CONCLUSIÓN

En definitiva, la verdadera innovación responsable y la defensa de la dignidad en la era digital, pilares del plan de la AEPD, exigen con urgencia tender un puente definitivo entre el mundo digital y el físico. No

se puede construir un futuro tecnológico ético y digno sobre los cimientos hundidos de una Administración pública que ignora la privacidad en sus interacciones más básicas con la ciudadanía. La desconexión actual no es solo una incongruencia legal; es una falla profunda en la concepción del Estado de derecho, que debe garantizar los derechos fundamentales en toda circunstancia. La implementación rigurosa de las medidas propuestas –desde el rediseño de espacios hasta un cambio radical en la cultura administrativa– no representa un simple gasto de adaptación logística, sino la inversión obligatoria en dignidad, confianza y calidad democrática. Liderar esta transformación, primero en España y luego como estándar europeo, sería el legado más perdurable y humano de la actual legislación de protección de datos, demostrando que el principio de privacidad desde el diseño debe aplicarse también al diseño de nuestra vida en común, asegurando que nadie tenga que elegir nunca entre su derecho a la intimidad y su derecho a la salud, al trabajo o a la justicia.

NORMATIVA CITADA

Agencia Española de Protección de Datos (2024). *Plan estratégico 2025-2030: Innovación responsable y defensa de la dignidad en la era digital*. https://www.aepd.es/la-agencia/plan-estrategico

Comité Europeo de Protección de Datos (2020). *Directrices 4/2019 sobre el artículo 25 del Reglamento (*UE*) 2016/679:Protecciódedatosdesdeeldiseñoypordefecto*(adoptadasel20deoctubrede2020).https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en

Consejo de Europa (2018). *Convenio 108+ para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, modificado por el Protocolo CETS núm. 223* (Estrasburgo, 10 de octubre de 2018). Instrumento de ratificación publicado en el *Boletín Oficial del Estado*, núm. 194, de 14 de agosto de 2023. https://www.boe.es/buscar/doc.php?id=BOE-A-2023-18506

Constitución española (1978). *Constitución Española*. *Boletín Oficial del Estado*, núm. 311, de 29 de diciembre de 1978). https://www.boe.es/buscar/act.php?id=BOE-A-1978-31229

España. Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales. *Boletín Oficial del Estado*, núm. 294, de 6 de diciembre de 2018). https://www.boe.es/eli/es/lo/2018/12/05/3/con

Parlamento Europeo y Consejo (2016). *Reglamento* (UE) *2016/679, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (*Reglamento General de Protección de Datos – *RGPD)*. *Diario Oficial de la Unión Europea*, L 119, pp. 1-88. http://data.europa.eu/eli/reg/2016/679/oj

Unión Europea (2000). *Carta de los Derechos Fundamentales de la Unión Europea*. *Diario Oficial de la Unión Europea*, C 364, 18 de diciembre de 2000, pp. 1-22). http://data.europa.eu/eli/treaty/char_2012/oj

Unión Europea (2016). *Directiva* (UE) *2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos, y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.*. *Diario Oficial de la Unión Europea*, L 119, pp. 89-131. http://data.europa.eu/eli/dir/2016/680/oj

Unión Europea (2022). *Reglamento* (UE) *2022/868 del Parlamento Europeo y del Consejo, de 30 de mayo de 2022, relativo a la gobernanza europea de datos y por el que se modifica el Reglamento* (UE) *2018/1724 (*Reglamento de Gobernanza de Datos – *Data Governance Act)*. *Diario Oficial de la Unión Europea*, L 152, pp. 1-44. http://data.europa.eu/eli/reg/2022/868/oj

RESOLUCIONES DE LA AEPD

Agencia Española de Protección de Datos (2020). Resolución de archivo de actuaciones E/07181/2019 (11 de agosto de 2020). https://www.aepd.es/documento/e-07181-2019.pdf

Agencia Española de Protección de Datos (2021). Resolución de archivo de actuaciones E/04967/2020. https://www.aepd.es/documento/e-04967-2020.pdf

Agencia Española de Protección de Datos (2021). Resolución de terminación del procedimiento por pago voluntario PS/00120/2021. https://protecciondata.es/wp-content/uploads/2023/04/ps-00120-2021.pdf

Agencia Española de Protección de Datos (2021). Resolución de procedimiento sancionador PS/00250/2021 de 1 de julio de 2021. https://www.iberley.es/resoluciones/resolucion-aepd-ps-00250-2021-01-07-2021-2394876

Agencia Española de Protección de Datos (2022). Resolución de procedimiento sancionador PS/00317/2022. https://www.aepd.es/documento/ps-00317-2022.pdf?LinkSource=PassleApp

RESOLUCIONES DEL TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA

Tribunal de Justicia de la Unión Europea (24 de noviembre de 2011). *Asociación Nacional de Establecimientos Financieros de Crédito* (ASNEF) *y Federación de Comercio Electrónico y Marketing Directo* (FECEMD), asuntos acumulados C-468/10 y C-469/10. ECLI:EU:C:2011:777.

Tribunal de Justicia de la Unión Europea (19 de octubre de 2016). *Patrick Breyer / Bundesrepublik Deutschland*, asunto C-582/14. ECLI:EU:C:2016:779.

REFERENCIAS BIBLIOGRÁFICAS

Altman, I. (1977). Privacy regulation: Culturally universal or culturally specific? *Journal of Social Issues*, *33*(3), 66-84. https://doi.org/10.1111/j.1540-4560.1977.tb01883.x

Antón, A. I., Earp, J. B. y Young, J. D. (2010). How internet users' privacy concerns have evolved since 2002. *IEEE Security & Privacy*, *8*(1), 21-27. https://doi.org/10.1109/MSP.2010.38

Arenas Ramiro, M. (2023). Las obligaciones de transparencia de las autoridades de protección de datos: un requisito indispensable para su independencia. *Revista Española de la Transparencia*, (17 extra), 227-270. https://doi.org/10.51915/ret.312

Bellanova, R. y González Fuster, G. (2013). Politics of disappearance: Scanners and (unobserved) bodies as mediators of security practices. *International Political Sociology*, *7*(2), 188-209. https://doi.org/10.1111/ips.12017

Burdon, M. y McKillop, A. (2013). *The Google Street View Wi-Fi scandal and its repercussions for privacy regulation* [Research Paper n.º 14-07]. University of Queensland TC Beirne School of Law. https://ssrn.com/abstract=2471316

Carazo Liébana, M. J. (2023). *El derecho fundamental a la protección de datos personales y la responsabilidad proactiva*. Aranzadi.

Cavoukian, A. (2009). *Privacy by design: The 7 foundational principles. Information and Privacy Commissioner of Ontario*, 5(2009).

Clarke, R. (2009). Privacy impact assessment: Its origins and development. *Computer Law and Security Review*, *25*(2), 123-135. https://doi.org/10.1016/j.clsr.2009.02.002

De Hert, P. y Papakonstantinou, V. (2016). The new General Data Protection Regulation: Still a sound system for the protection of individuals? *Computer Law & Security Review*, *32*(2), 179-194. https://doi.org/10.1016/j.clsr.2016.02.006

Edwards, L. y Veale, M. (2017). Slave to the algorithm? Why a «right to an explanation» is probably not the remedy you are looking for. *Duke Law & Technology Review*, (16), 18-84. https://scholarship.law.duke.edu/dltr/vol16/iss1/2

Flores Cabrera, F. (2023). *La protección de datos personales como límite al acceso a la información pública: las condiciones de un equilibrio necesario* [trabajo de fin de máster]. Universitat de Barcelona. https://hdl.handle.net/2445/202529

González Fuster, G. (2014). *The emergence of personal data protection as a fundamental right of the EU*. Springer. https://doi.org/10.1007/978-3-319-05023-2

González Suárez, G. M. (2025). *Régimen jurídico de la protección de datos relacionados con la salud* [tesis doctoral]. Universidad de Oviedo. https://hdl.handle.net/10651/81113

Hijmans, H. (2016). The mandate of the EU under Article 16 TFEU and the perspectives of legitimacy and effectiveness. En *The European Union as guardian of internet privacy: The story of Art. 16 TFEU* (pp. 125-183). Springer Cham.

Kosta, E. (2013). *Consent in European data protection law* [Nijhoff Studies in EU Law, 3]. Brill y Nijhoff.

Lynskey, O. (2015). *The foundations of EU data protection law*. Oxford University Press.

Lyon, D. (2018). *The culture of surveillance: Watching as a way of life*. Polity Press.

Nissenbaum, H. (2009). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press.

Pedraza Córdoba, J. (2023). *Responsabilidad proactiva en la gestión de datos personales por administraciones públicas*. Tirant lo Blanch.

Piñar Mañas, J. L. (2014). Transparència i dret d'accés a la informació pública. Algunes reflexions al voltant del dret d'accés a la Llei 19/2013, de transparència, accés a la informació i bon govern. *Revista Catalana de Dret Públic*, (49), 1-19. https://doi.org/10.2436/20.8030.01.29

Puerta Domínguez, E. M. (2023). El marco jurídico de la Unión Europea sobre protección de datos y garantías ciudadanas ante la Administración pública electrónica. *Ius et Scientia*, *9*(1), 23-45. https://doi.org/10.12795/IESTSCIENTIA.2023.i01.03

Reding, V. (2011). The upcoming data protection reform for the European Union. *International Data Privacy Law*, *1*(1), 3-5. https://doi.org/10.1093/idpl/ipq007

Ridaura Martínez, M. J. (2021). Los derechos fundamentales como límites en el marco de la investigación privada. *Teoría y realidad constitucional*, (47), 129-159. https://doi.org/10.5944/trc.47.2021.30710

Rodríguez Roca, A. (2022). *La protección de datos personales en los juzgados y tribunales. Un enfoque desde la perspectiva laboral*. La Ley.

Solove, D. J. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review*, *154*(3), 477-564. https://doi.org/10.2307/40041279

Zuboff, S. (2015). Big other: Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, *30*(1), 75-89. https://doi.org/10.1057/jit.2015.5