EDICIONES
COMPLUTENSE

Derecom
e-ISSN 1988-2629

ARTÍCULOS

Administración inteligente de datos: habemus Omnibus Digital UE

Mª Pilar Dopazo Fraguío
Universidad Complutense de Madrid (España)

https://dx.doi.org/10.5209/dere.108559 Recibido: 22/03/2026 • Revisado: 06/04/2026 • Aceptado: 24/04/2026

Resumen: En este trabajo es objeto de valoración el denominado paquete normativo Ómnibus Digital presentado por la Comisión Europea. Siendo un tema de suma actualidad, plantea varias cuestiones jurídicas sobre las que conviene profundizar. Por ello, son analizadas las principales modificaciones regulatorias que han sido propuestas, con la finalidad -en principio- de facilitar el emprendimiento digital e inteligente y dinamizar la competitividad en el mercado UE creado en torno a los datos, como valioso activo hoy reconocido. Dicho interés, a su vez, responde a los propios objetivos de la Estrategia europea emprendida y, con ello, a la necesidad de "reconfigurar" la normativa vigente en esta materia, también ante el posicionamiento fáctico de la inteligencia artificial (IA). No obstante, parece oportuno reflexionar acerca de las reformas legales proyectadas; en especial, observando su incidencia en el vigente marco regulatorio que rige la protección de datos personales de forma específica, entre otras tipologías de datos que pudieran verse afectadas. Los cambios planteados son significativos, al afectar a varias leyes UE, en virtud de las cuales se había logrado consolidar un avanzado Sistema jurídico común aplicable a la gestión del dato, dinámico y de distinta tipología. En este sentido, se infiere que, más allá del buen propósito del legislador europeo, algunas de las innovaciones propuestas sí inciden en las bases sólidas ya construidas por el Ordenamiento, incluso, poniendo en jaque al deber de tutela pública que corresponde a derechos reconocidos como fundamentales y a las garantías ofrecidas.
Palabras clave: Ómnibus digital; modificaciones normativas; Estrategia europea y mercado de datos; inteligencia artificial; protección de datos.

EN Smart data management: habemus Omnibus Digital UE

Abstract: In this paper we assess the so-called Digital Omnibus package presented by the European Commission. This highly topical issue raises several legal questions that warrant further examination. Therefore, the main proposed regulatory changes are analyzed, with the primary aim of facilitating digital and smart entrepreneurship and boosting competitiveness in the EU market built around data, now recognized as a valuable asset. This interest, in turn, aligns with the objectives of the European Strategy and, consequently, with the need to reconfigure existing regulations in this area, particularly given the established presence of artificial intelligence (AI). However, it seems appropriate to reflect on the proposed legal reforms, especially considering their impact on the current regulatory framework governing the protection of personal data, among other types of data that could be affected. The proposed changes are significant, affecting several existing EU laws that had established an advanced common legal framework for managing dynamic data of various types. In this respect, it can be inferred that, despite the European legislator's good intentions, some of the proposed innovations could indeed undermine the solid foundations already built by the legal system, even jeopardizing the public duty to protect fundamental rights and the guarantees offered.
Keywords: Omnibus digital; legal changes; European strategy and digital data market; artificial intelligence; data protection.

Sumario: 1. Introducción. 2. El Sistema jurídico vigente UE: marco regulatorio básico y común preexistente en materia de datos. 3. El nuevo "paquete normativo Ómnibus digital": objetivos y principales características del nuevo enfoque regulatorio. 3.1. Principales objetivos. 3.2. Principales reformas regulatorias. 4. Consideraciones de especial relevancia desde la óptica del Derecho administrativo y en atención al contexto digital con la incorporación de la IA. 4.1. El deber de tutela pública reforzada en el caso de derechos

fundamentales, protección de datos y privacidad. 4.2. La protección de otros derechos y tipologías de datos (datos no personales). 5. Conclusiones. Notas. Referencias bibliográficas.

Cómo citar: Dopazo Fraguío, M.P. (2026). "Administración inteligente de datos: habemus Omnibus Digital UE". *Derecom,* 39(1), 3-20. DOI: https://dx.doi.org/10.5209/dere.108559

1. Introducción. Objetivos del estudio y metodología

La Comisión Europea ha encaminado, en la actualidad, una ambiciosa reforma del marco regulatorio vigente en materia de derecho digital. Las innovaciones jurídicas propuestas conllevan cambios normativos muy significativos, afectando, en particular, a la disciplina establecida en lo relativo a la gestión y el tratamiento de los datos. El nuevo enfoque legal ha sido planteado, en principio, con la finalidad de facilitar el cumplimiento normativo, incentivar la competitividad de las empresas y promover el desarrollo de sistemas basados en inteligencia artificial (IA).

Así se observa, con motivo de la presentación de la propuesta del paquete normativo denominado "Ómnibus Digital", realizada por la Comisión Europea el 19 de noviembre de 2025[1]. Con dicha iniciativa legislativa, se pretende revisar y simplificar el régimen jurídico preexistente aplicable en materia de datos -personales y no personales-, inteligencia artificial y ciberseguridad. De este modo, se trataría de facilitar la aplicación efectiva de la legislación digital vigente, común y aplicable en el Ordenamiento jurídico europeo.

A dichos objetivos se propone revisar el marco regulatorio digital para su posible simplificación y con ello, a su vez, asegurar su eficaz aplicación en la Unión Europea (UE). En concreto, dicho bloque regulatorio queda integrado por dos propuestas principales de Reglamentos (UE): "Ómnibus Digital sobre el Acervo Digital" y "Ómnibus Digital sobre IA".

El propósito principal del legislador europeo, vía estos instrumentos normativos, sería adaptar la actual normativa ante los nuevos retos que han sido identificados o previstos en materia de datos, IA y ciberseguridad; asimismo, procurar facilitar los objetivos marcados por la Estrategia de datos y la competitividad en el mercado digital diseñado. Con estas finalidades, se introducen varias modificaciones en normas consolidadas, las cuales, hasta la fecha, han sido estimadas como pilares clave del Derecho UE en este campo. Tales son el Reglamento General de Protección de Datos (RGPD, en adelante)[2], el Reglamento de Gobernanza de Datos (Data Governance Act, 2022)[3] y el Reglamento sobre normas armonizadas para un acceso justo a los datos y su utilización (Data Act, 2023)[4], el Reglamento de Inteligencia Artificial (Artificial Intelligence Act, 2024)[5], entre otras que también son reseñadas a continuación en este texto.

Resulta evidente el cambio de enfoque propuesto, a la vista de la pretensión enunciada por la Comisión Europea y observando los contenidos propuestos mediante el citado Ómnibus Digital, tal y como de forma ulterior es examinado en este texto. Al respecto, entre las novedades actuales más relevantes, hay que destacar una trascendental, por lo que concierne al RGPD, esta es la redefinición interpretativa de la noción de datos personales. Y, por otra parte, otras aportaciones son aquellas relativas a la simplificación administrativa, como es -por ejemplo- el establecimiento de un punto único de notificación de incidentes de ciberseguridad. También, otras medidas que modifican algunos aspectos regulados por el más reciente Reglamento de IA. Con relación a este último, se introducen nuevas reglas en orden a facilitar el empleo de herramientas de IA y los plazos otorgados para su implementación. De igual modo, se promueve los *sandboxes* regulatorios[6] (entornos seguros y controlados para la realización de pruebas o prácticas experimentales de nuevas tecnologías, la prestación de servicios o fórmulas de negocio)[7]. A su vez, en este terreno, son efectuadas otras reformas destacadas en lo relativo a los deberes que corresponde cumplir a los responsables del tratamiento de datos, entre otros sujetos. Estas acciones facilitadoras estarían

1 Comisión Europea: Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se modifican los Reglamentos (UE) 2016/679, (UE) 2018/1724, (UE) 2018/1725, (UE) 2023/2854 y las Directivas 2002/58/CE, (UE) 2022/2555 y (UE) 2022/2557 en lo que respecta a la simplificación del marco legislativo digital, y se derogan los Reglamentos (UE) 2018/1807, (UE) 2019/1150, (UE) 2022/868 y la Directiva (UE) 2019/1024 (Ley Ómnibus Digital). Bruselas, 19.11.2025. COM/2025/837 final. Asimismo, vid., https://digital-strategy.ec.europa.eu/es/library/digital-omnibus-regulation-proposal; y, https://ec.europa.eu/commission/presscorner/detail/es/ip_25_2718 (Fecha última consulta: 14/03/2026).

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 y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). DOUE L 119, de 4.5.2016.

3 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). DOUE L 152, de 3 jun. 2022.

4 Reglamento (UE) 2023/2854 del Parlamento Europeo y del Consejo de 13 de diciembre de 2023 sobre normas armonizadas para un acceso justo a los datos y su utilización, y por el que se modifican el Reglamento (UE) 2017/2394 y la Directiva (UE) 2020/1828 (Reglamento de Datos). DOUE L 2854, de 22.12.2023.

5 Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo de 13 de junio de 2024 por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n.° 300/2008, (UE) n.° 167/2013, (UE) n°.168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial). DOUE L de 12.7.2024.

6 Acerca de los *sandboxes* regulatorios, vid., Rodríguez Cembellín, D. (2025): Los sandboxes regulatorios y su uso en la regulación de la inteligencia artificial. *Revista General de Derecho Administrativo*, 70. Aguilar Alonso, I. y Lluesma Rodrigo, P. (2019): Una introducción al sandbox regulatorio, *Actualidad jurídica Uría Menéndez*, 52, pp. 95-100. https://www.uria.com/documentos/publicaciones/6676/documento/foro05.pdf?id=8961&forceDownload=true (fecha consulta: 10/02/2026).

7 *Sandboxes:* entornos controlados de pruebas, vid., definición y aspectos aplicativos, en: https://www.ciencia.gob.es/Innovar/SandBoxes.html (Fecha consulta: 14/03/2026).

destinadas, de forma principal -según lo previsto-, a determinadas empresas, pymes y entidades calificadas como *mid-caps* o empresas de capitalización media *(empresas cotizadas cuya capitalización bursátil es estimada de mediana dimensión en comparación con* otras sociedades cotizadas).

Dado el notable interés de las innovaciones planteadas, en este trabajo son expuestas de forma específica, ofreciendo una síntesis de sus implicaciones técnicas y jurídicas. En todo caso, antes de ofrecer cualquier valoración sobre lo propuesto, digno es -en esta introducción- poner en valor la normativa europea vigente en materia de datos. Toda vez que hoy nos ha permitido contar con un marco jurídico sólido, preceptivo y común en la UE. En este sentido, hay que reconocer cómo el mismo ha progresado, de forma muy positiva, en las últimas décadas y, en particular, desde que fuera adoptado el RGPD por lo que respecta a la protección de los datos personales. También en los últimos años, cuando han sido aprobados otros actos normativos UE de suma relevancia, como son los precitados, vigentes en estos momentos. Así, en especial, cabe hacer hincapié en los avances procurados en lo relativo a cuestiones como son los datos abiertos, la reutilización de la información y el sistema de gobernanza del dato. Gracias a lo cual, por tanto, se ha logrado disponer -hasta la fecha- de un completo régimen jurídico, como ha sido manifestado por la doctrina científica[8]. Incluso, ofreciendo un modelo europeo muy ilustrativo para otros ordenamientos de terceros países.

Ahora bien, una vez reconocido lo anterior, lo cierto es que, en el presente, asistimos a lo que podría ser un cambio en la orientación o el rumbo normativo. Esto es, a tenor de lo anunciado por la Comisión Europea y según lo planteado por las nuevas propuestas, se produciría un giro importante en el enfoque regulatorio. Ello implicaría la reformulación del modelo jurídico acuñado, lo cual, *per se*, no es baladí, como se argumenta en este texto.

Dicha "renovación" emprendida de la normativa vigente respondería al interés europeo de lograr ser más competitivos en el mercado digital de los datos. O, en suma, en la pretensión de incrementar el liderazgo UE ante el paradigma económico que ha sido trazado en torno al dato. Sin duda, en el escenario actual, resulta evidente el valor adquirido por los datos, al ser apreciados como activo intangible clave, cada vez más valorado. Pues, además, se trata de un recurso básico o materia prima nuclear para el funcionamiento operativo de la IA, amén de su necesario entrenamiento previo, al fin de posibilitar la proyección aplicativa de esta tecnología emergente en los distintos ámbitos o sectores. Por ende, admitiendo esta realidad, se razona el creciente posicionamiento del valor económico o mercantil alcanzado por los datos, o por el "dato de calidad" como intangible, cuya *vis* atractiva se incrementa de forma progresiva en los ecosistemas digitales, en lógica congruencia con el alto potencial que ofrece o su utilidad instrumental.

De ahí, ahora, bien se explica el interés que subyace cuando se proponen cambios regulatorios radicales, como son los proyectados. En este sentido, según se infiere, su finalidad fundamental sería estratégica, orientando la configuración de un nuevo sistema jurídico destinado -de forma esencial- a promover una mayor disponibilidad de datos accesibles y dinámicos, su libre circulación, uso o reutilización.

Por ende, el propósito facilitador sería el denominador común que inspira la reforma planteada, incrementando el acceso y el tráfico de los datos (digitalizados) en el mercado digital UE[9]. Todo ello, a su vez, respondería a los objetivos de la Estrategia Europea de Datos[10]. Por consiguiente, teniendo en cuenta lo señalado y desde la perspectiva jurídica, cabe entender el giro europeo observado. Toda vez que el actual propósito de la Comisión Europea se centra en estos aspectos, más que en otros antes considerados como prioritarios, por ejemplo, lo relativo a la protección de datos personales o de otro tipo.

Ello*, a priori*, se infiere, a la luz de la renovación normativa propuesta y objeto de estudio. No obstante, conviene profundizar en las nuevas propuestas normativas, también en atención a los argumentos que motivarían la pretendida reconfiguración actual de la legislación UE precitada. Así pues, considerando como punto de partida las premisas enunciadas, son identificados dos objetivos como auténticos motores impulsores de la reforma legal planteada: configurar un marco regulatorio europeo más facilitador y procurar mayor simplificación administrativa[11].

Expuesto lo anterior, el presente artículo -fruto del previo estudio de investigación realizado en esta materia- tiene como propósitos aproximar el

---

8 Como la doctrina ha señalado, la protección de datos constituye un derecho fundamental imprescindible y, como tal, requiere disponer de óptimas garantías. Entre otros autores, vid., J.L. Piñar Mañas, J.L. (2020): Las claves de un derecho fundamental imprescindible. *El Cronista del Estado Social y Democrático de Derecho*, 88-89 (Ejemplar dedicado a: Protección de datos: antes, durante y después del coronavirus), pp. 6-19. Y, el trabajo más reciente, Piñar Mañas (2025): ¿*Quo vadis,* protección de datos?. *Revista de privacidad y derecho digital*, vol. 10, 36, pp. 19-24.

9 Sobre esta cuestión, en concreto, vid., Dopazo Fraguío, M.P. (2025): Tráfico digital de datos: Consideraciones sobre la actual cobertura legal europea. ¿Tutela pública suficiente?, en Candelario, M.I. (dir.), *La propiedad industrial entre la digitalización, la innovación y la sostenibilidad.* Tirant lo Blanch, Valencia 2025 (Capítulo 6, págs. 143-197). https://doi.org/10.36151/TLB_9791370109493

10 Comisión Europea: Comunicación de 19 de febrero de 2020 sobre una Estrategia Europea de Datos. Cfr., Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, *Configurar el futuro digital de Europa,* Bruselas, 19.2.2020 COM (2020) 67 final. https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52020DC0067.

11 En los últimos años se ha producido un notable incremento de los canales digitales y servicios virtuales ofrecidos, lo cual también afecta a las vías empleadas por las Administraciones públicas para relacionarse entre sí o con otras entidades o sujetos. De igual modo, esta realidad, incide de forma especial en la relación con la ciudadanía. En efecto, se produce lo que podría calificarse como un proceso evolutivo hacia la virtualización administrativa, lo cual, también se observa por lo que respecta a la atención prestada por parte de la Administración. Al respecto, Cerrillo i Martínez, A., dir. (2022): *La administración digital.* Dykinson, Madrid. Y, el trabajo de Moro Cordero, M.A. y Cerrillo i Martínez, A. (2024): El nuevo Reglamento sobre la Europa interoperable en el marco de la estrategia europea de datos. *Consultor de los ayuntamientos y de los juzgados: Revista técnica especializada en administración local y justicia municipal*, 9.

conocimiento sobre las nuevas propuestas normativas planteadas en el Ordenamiento común europeo, así como aportar un análisis con finalidad iusinformativa sobre el actual paquete normativo "Ómnibus Digital UE" presentado por la Comisión Europea. Asimismo, al respecto, se ofrece una valoración reflexiva sobre las principales implicaciones técnicas y jurídicas de la normativa proyectada.

En particular, con el trabajo efectuado -conforme a la metodología científica propia de los estudios doctrinales- se pretende destacar aquellas novedades más relevantes, subrayando las modificaciones legales previstas y examinando sus posibles efectos. Toda vez que se estima de gran importancia la reforma legal planteada, al suponer un cambio radical en el enfoque legal precedente. Dichas innovaciones -como se aborda de forma específica- afectan al tratamiento de los datos y, en consecuencia, comportarían una alteración sustancial de las bases normativas. Esto es, aquellas sobre las que se sustenta la estructura del vigente Sistema jurídico UE aplicable a los datos. Con esta motivación, se argumenta el interés del estudio, el examen de las innovaciones jurídicas propuestas desde la Comisión y, en atención a ellas, la exposición razonada de algunas consideraciones preliminares.

Asimismo, lo señalado puede resultar muy oportuno en estos momentos, estando pendientes de la tramitación legislativa que procederá. Por lo cual, conviene subrayar el potencial impacto que conllevaría adoptar los cambios propuestos y no ignorar sus riesgos. Observándose, en este sentido, cómo lo planteado sí incide de forma sustancial en el actual modelo regulatorio que rige la gobernanza y el positivo tratamiento de los datos. Y, en particular, por lo que respecta a determinados aspectos muy significativos, al afectar a cuestiones muy sensibles, como es todo lo relativo a la tutela otorgada a los datos y según su tipología. De igual modo, en orden al deber exigible de brindarles una óptima salvaguarda; esto es, de acuerdo con las obligaciones de tratamiento impuestas hasta la fecha, de conformidad con la actual legislación. Y, desde luego, teniendo presente, de forma específica, aquellos deberes requeridos en el caso de determinadas categorías de datos, por ejemplo, datos personales o información relacionada con la la privacidad de los ciudadanos, entre otros supuestos. Toda vez que estas cuestiones constituyen hoy por hoy -como se sabe- derechos fundamentales consagrados por el Derecho.

2. El Sistema jurídico vigente UE: marco regulatorio básico y común preexistente en materia de datos.

Considerando todo lo expuesto supra, resulta patente el interés actual que, por su valor como activo intangible, adquieren los datos de distinta tipología o aquellos de categoría especial. Esto, también, es apreciado por los operadores y en el mercado digital UE[12]. A su vez, observando que se trata de un necesario recurso indispensable- para el entrenamiento y el eficaz funcionamiento de la IA. De ahí, como ha sido avanzado, bien se explica el actual interés europeo en tratar de revisar el actual marco normativo aplicable en materia de tratamiento de datos, así como, en orden a facilitar su cumplimiento, además de incorporar medidas que posibiliten la implementación de esta tecnología. Todo ello, por tanto, ha sido encaminado en pos de avanzar en los objetivos trazados por la Estrategia UE de datos y el mercado digital.

Ahora bien, también por estos mismos motivos, conviene tener presente la normativa vigente en materia de protección de datos y, a su vez, reforzar todo lo relativo a su deber de tratamiento eficaz. Por lo cual, en este sentido -en nuestra opinión-, no debería reducirse en ningún caso el nivel de protección que se ha logrado alcanzar, conforme al ya consolidado marco regulatorio europeo. Razón por la cual, en este epígrafe del texto -y antes de abordar las innovaciones propuestas a raíz de Ómnibus Digital-, aportamos expresa referencia a la vigente legislación europea, centrando nuestra atención en los aspectos nucleares que rigen en este campo.

En este sentido, cabe esgrimir que, ante las innovaciones planteadas a raíz del Ómnibus Digital, ha de tenerse en cuenta -en coherencia o buena lógica- todo lo ya logrado por el Ordenamiento UE. Esto es, la disciplina consolidada en el actual régimen jurídico adoptado en lo relativo a la protección de datos y la gobernanza del dato. Más aún a futuro, dada la complejidad del contexto digital descrito, así como los eventuales riesgos de la acelerada proyección tecnológica que acontece. Por tanto, parece que lo prudente sería -en términos preventivos- reforzar las medidas destinadas a optimizar la gestión de datos. Considerando así que, en todo caso, esta cuestión debería ser enfocada como un aspecto indispensable en toda organización o entidad. Su implementación, en la práctica, ha de ser integral y efectiva, quedando vinculada, a su vez, a la gestión del riesgo[13]. Por cuanto ambos elementos constituyen presupuestos estratégicos requeridos, asimismo, esenciales a efectos de acreditar el debido cumplimiento regulatorio. Y ello, por ende, no ha de mermar -o no debería- aunque se trate de promover el desarrollo de la IA y la competitividad en el mercado digital.

No obstante, estas premisas básicas podrían no ser las que ahora primarían, lo que se infiere de la Comunicación de la Comisión Europea al Parlamento Europeo y al Consejo: *Estrategia para una unión de datos- Desbloqueo de datos para la IA*, de 19 de noviembre de 2025[14]. Bruselas, 19.11.2025, COM/2025/835 final. Y, en la actualidad, en concreto, a la vista de algunas de las propuestas de

[12] En este mismo sentido, vid., López-Lapuente, L. (2023): La nueva regulación europea de los datos: cómo dar forma al futuro digital de Europa". *Actualidad Jurídica Uría Menéndez*, 61, pp. 50-71. https://www.uria.com/documentos/publicaciones/8346/documento/AJUM_61.pdf?id=13294&forceDownload=true (Fecha consulta: 10/01/2026).

[13] Con respecto a este aspecto señalado, resulta ilustrativa la guía facilitada por la Agencia Española de Protección de Datos (AEPD), "Gestión del riesgo y evaluación de impacto en tratamientos de datos personales", 29 de junio de 2021. Disponible en: https://www.aepd.es/guias/gestion-riesgo-y-evaluacion-impacto-en-tratamientos-datos-personales.pdf (Fecha consulta:10/02/2026).

[14] Cfr., Comunicación de la Comisión Europea al Parlamento Europeo y al Consejo: *Estrategia para una unión de datos –Desbloqueo de datos para la IA*. Bruselas, 19.11.2025, COM/2025/835 final, en: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52025DC0835

modificación de la normativa vigente que han sido realizadas vía el Ómnibus Digital, como detallamos en el siguiente epígrafe 3.2.

Por ello, ante todo, conviene recordar que, en materia de datos y de acuerdo con la legislación vigente, se ha de actuar conforme al establecido principio de proactividad responsable[15]. Y como tal, esto es exigible a todo operador, según nuestro Ordenamiento UE. Lo señalado obliga al tratamiento diligente de los datos de distinta tipología, personales y no personales, entre otros deberes. En consecuencia, lógico es estimar que el genuino y actual Sistema jurídico de protección de los datos personales (RGPD, 2016) y el Sistema integral de gobernanza del dato (2022) debieran seguir siendo considerados ejes básicos del marco regulatorio que dicta la disciplina a seguir, tal y como se preceptúa por el legislador europeo.

Estas premisas pudieran ser principales ante las posibles o nuevas reformas regulatorias que se plantean. Pues, desde nuestra óptica jurídica, difícil justificación podría encontrar una reforma legal que suponga reducir las garantías alcanzadas en este campo, o, en concreto, una eventual disminución de las obligaciones de tratamiento que corresponden a todo operador o responsable de datos. Toda vez que, como cabe entender, deben ser preservados los derechos relativos a la protección de los datos. Máxime, ante el raudo desarrollo de las nuevas herramientas tecnológicas o la aplicación de sistemas de IA.

En este sentido, por tanto, pudiera ser más recomendable tratar de conciliar derechos e intereses en justo equilibrio. Esto es, en nuestra opinión, se ha de poder equilibrar el derecho a la protección de datos con el pretendido progreso tecnológico, la innovación y el fomento de la competitividad en el mercado digital. Pues, promover estos últimos no ha de afectar a la tutela otorgada al dato.

De cualquier modo, hoy por hoy, los principios dictados por la UE que han de regir en el terreno aplicativo de la gobernanza del dato son los establecidos por la legislación vigente. Ello, precisamente, ha sido disciplinado con el fin de generar mayor confianza y seguridad jurídica en este campo, vía dos Reglamentos europeos (precitados), siendo así los pilares básicos normativos en esta materia, a saber, el Reglamento UE sobre Gobernanza de datos (*Data Governance Act,* 2022) y el Reglamento UE de Datos (*Data Act,* 2023). Este último, a su vez, complementa al primero e incorpora novedades relevantes[16]. Debiendo, por su parte, atender a lo preceptuado por el RGPD, como así queda precisado en dichas Leyes UE.

La innovación legal que aporta esta regulación preexistente -y vigente de forma plena, en la actualidad- ha sido clave en este terreno, por lo que su examen a fecha actual resulta fundamental y en orden a poder orientar futuras propuestas. En este trabajo, en concreto, destacamos estas Leyes UE, también por las aportaciones técnicas que conllevan, significando su máximo valor jurídico. De este modo, son examinadas observando su relevante impacto, más aún considerando su carácter vinculante y con aplicación directa en toda la UE -al tratarse de Reglamentos UE-, también teniendo en cuenta el amplio ámbito subjetivo y objetivo que las identifica. Analizar estas y otras características específicas es principal para identificar la innovación jurídica aportada, así como evaluar su potencial proyección. De igual modo, con el fin de evaluar las posibles implicaciones prácticas que conlleva en la actualidad.

Ergo, su debida observancia resulta esencial en aras de asegurar un óptimo grado de *compliance* legal. Además, la segunda Ley UE citada, *Data Act*, resulta de igual modo muy relevante, al operar como normativa complementaria de la primera, pues aporta una regulación adicional a lo previsto en el Reglamento sobre gobernanza del dato o *Data Governance Act*. Por este motivo, se considera que el Reglamento del Dato (2023) es un complemento regulatorio necesario al previo Reglamento de Gobernanza (2022).

Asimismo, adviértase que el vigente *Data Act* (2023) ya ha supuesto un giro relativo en esta materia, toda vez que se adoptó con la finalidad de que la regulación previa impuesta pudiera ser más flexible o propiciadora con respecto a la disponibilidad de algunas tipologías de datos. Esto es, para que, en la práctica, pudiera estar más en consonancia con las necesidades o demandas de la economía digital europea. De este modo, en concreto, se ampliaban las posibilidades para acceder a datos de interés, como aquellos que -por ejemplo- fueran generados por productos o servicios inteligentes, equipos o dispositivos conectados. También, se prohíben ciertas prácticas abusivas, y se facilita la portabilidad de datos. Entre otras medidas aplicables, ya queda previsto lo relativo a la protección de la información ante eventuales actuaciones ilícitas de determinados operadores de terceros países.

En suma, las "Leyes UE" precitadas están vigentes y configuran pilares normativos, al dictar las bases del actual Sistema regulatorio aplicable en esta materia. Y, como tales, en la práctica, han de ser consideradas e interpretadas de forma conjunta. Ello, sin perjuicio del valor de otros actos normativos previos -también hoy vigentes- como son aquellos específicos aplicables en materia de protección de datos

[15] En este sentido, se ha pronunciado la jurisprudencia y de forma expresa el TEDH. Al respecto, vid., Barnés Vázquez. J. (1998): El principio de proporcionalidad. *Cuadernos de Derecho Público* - Instituto Nacional de Administración Pública, 5. Recuperado a partir de https://revistasonline.inap.es/index.php/CDP/article/view/509 (Fecha consulta: 11/02/2026). Y, sobre el principio de proporcionalidad y los "supraprincipios" que inspiran la aplicación e interpretación del RGPD, legitimidad, proporcionalidad, empoderamiento, transparencia, responsabilidad proactiva y seguridad, vid., Barrio Andrés, M. (2024): Los principios estructurales del Reglamento General de Protección de Datos. *Actualidad jurídica iberoamericana*, 20, 2024, pp. 1322-1341. Disponible en: https://revista-aji.com/wp-content/uploads/2024/02/AJI20_Art_42.pdf. Asimismo, con carácter previo, han sido analizados con detalle este y otros principios rectores, entre otros presupuestos que se consolidan en el Derecho de la UE en virtud del RGPD, véase, Dopazo Fraguío, P. (2019): Protección de datos y derechos digitales: arquitectura del nuevo binomio regulatorio. *Derecom*, 26, 2019, pp. 17-48.

[16] De forma específica, para mayor detalle sobre el Sistema jurídico europeo de gobernanza de datos, véase el estudio específico realizado por Dopazo Fraguío, P. (2022): El nuevo reglamento europeo para la gobernanza del dato: ¿Liberación segura de información y neutralidad de su tratamiento?". *REDE, Revista española de derecho europeo*, 82, 2022, pp. 115-166.

personales[17]: el Reglamento Europeo en materia de protección de datos personales (RGPD 2016)[18] y, su complementario, el Reglamento relativo a un marco para la libre circulación de datos no personales en la Unión Europea (2018)[19].

Junto a estas normativas vigentes que han sido referenciadas, se añade otra ulterior de interés en este campo -si bien, no exenta de polémica-[20] como es el Reglamento (UE) 2025/327, del Parlamento Europeo y del Consejo, de 11 de febrero de 2025, relativo al Espacio Europeo de Datos de Salud, y por el que se modifican la Directiva 2011/24/UE y el Reglamento (UE) 2024/2847[21]. Por tanto, quedando también previsto la posible incorporación de herramientas basadas en IA en el ámbito del espacio digital de salud, también el tratamiento de datos es -y ha de ser, en todo caso- aspecto esencial a tener en cuenta.

Por último, hay que mencionar, dentro del primer paquete o conjunto de normas que desarrollan el actual texto del RGPD, el recientemente adoptado Reglamento (UE) 2025/2518 del Parlamento Europeo y del Consejo, de 26 de noviembre de 2025, por el que se establecen normas procedimentales adicionales sobre la garantía del cumplimiento del Reglamento (UE) 2016/679[22]. El objeto de este nuevo Reglamento son normas procedimentales, por lo que su funcionalidad es adicional al RGPD, al regular el procedimiento aplicable en supuestos de conflictos derivados del tratamiento transfronterizo de datos personales. A dichos efectos, se establece la vía de tramitación y lo referente a la intervención de las autoridades de control o supervisión. Incluso, quedando prevista la actuación del Comité Europeo de Protección de Datos (CEPD). También, en estos casos, se determina el posible ejercicio de los derechos reconocidos a las partes. Por tanto, básicamente, con este texto legal se concreta el procedimiento y las competencias de las autoridades supervisoras ante estos eventos. De este modo, se unifican los criterios para decidir sobre si un asunto planteado constituye -o no- una controversia relativa al tratamiento transfronterizo de datos de esta tipología y, en dicho caso, cómo ha de proceder la tramitación de las reclamaciones que fueran presentadas, las actuaciones de investigación que correspondería practicar y las autoridades administrativas de control que en materia de tratamientos son competentes.

Con todo, una vez descrito el contexto técnico y regulatorio donde nos ubicamos en el presente, el estudio se centra, a continuación, en el examen de las nuevas propuestas normativas contenidas en el actual Ómnibus Digital. Ello, con el fin de destacar sus objetivos, principales novedades e implicaciones jurídicas. Al respecto, cabe avanzar -por su relevancia- que una de las cuestiones que ya ha despertado cierta inquietud y, por ello, ocupa el debate doctrinal actual, es la posible redefinición de la genuina noción legal de "dato o datos personales" prevista por el RGPD. Toda vez que con motivo de las modificaciones anunciadas -y por lo que respecta a este texto legal aprobado en 2016-, podría ser reconfigurado dicho concepto o su posible interpretación, lo cual, en la práctica, podría conllevar el debilitamiento de la protección de datos. En este sentido, además, es reseñable lo que ha sido manifestado en el Dictamen conjunto adoptado el 10 de febrero de 2026, emitido por el Comité Europeo de Protección de Datos (CEPD) -*European Data Protection Board* (EDPB), en inglés- y el Supervisor Europeo de Protección de Datos (SEPD)[23]. En dicho

---

17 En particular, con referencia al derecho fundamental a la protección de datos personales y sobre la legislación común europea aplicable en esta materia, así como la complementaria nacional en nuestro país, vid., entre otros trabajos, Dopazo Fraguío, P. (2019): Protección de datos y derechos digitales: arquitectura del nuevo binomio regulatorio. *Derecom: Revista Internacional de Derecho de la Comunicación y las Nuevas Tecnologías*, 26, pp. 17-48. López Calvo, J., coord. (2019): *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD*. Wolters Kluwer España, Madrid. Barrio Andrés, M. (2024); Los principios estructurales del Reglamento General de Protección de Datos. *Actualidad jurídica iberoamericana*, 20, 2024, pp. 1322-1341. Disponible en: https://revista-aji.com/wp-content/uploads/2024/02/AJI20_Art_42.pdf. Asimismo, sobre su evolución y perspectie vas de proyección, el estudio realizado por Pérez de los Cobos Orihuel, F. (2018): *El derecho al respeto de la vida privada: los retos digitales, una perspectiva de Derecho comparado. Consejo de Europa*. EPRS, Servicio de Estudios del Parlamento Europeo, Bruselas, 2018. Disponible en: https://www.europarl.europa.eu/RegData/etudes/STUD/2018/628261/EPRS_STU(2018)628261_ES.pdf (Fecha consulta: 20/02/2026). Piñar Mañas, J.L. (2025): *¿Quo vadis,* protección de datos?, *Revista de privacidad y derecho digital*, 36, pp. 19-24.

18 En especial, en materia de protección y tratamiento de "datos personales" hay que tener presente el RGPD: Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). DOUE L n.º 119, de 4.5.2016. Asimismo, vid., en nuestro país, la legislación nacional, 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). Y, la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales (BOE núm. 126, de 27 de mayo de 2021).
Al respecto, también puede ser consultada, la guía facilitada por la Agencia Española de Protección de Datos (2018): "Guía del Reglamento General de Protección de Datos para responsables de tratamiento". AEPD, Madrid. Disponible en: https://www.aepd.es/media/guias/guia-rgpd-para-responsables-de-tratamiento.pdf (Fecha consulta: 15/02/2026).

19 Con respecto a la libre circulación de "datos no personales", vid., Reglamento (UE) 2018/1807 del Parlamento Europeo y del Consejo de 14 de noviembre de 2018 relativo a un marco para la libre circulación de datos no personales en la Unión Europea. DOUE L n.º 303, de 28.11.2018.

20 Como ha sido puesto de relieve por la doctrina administrativista, Valero Torrijos, J. (2023): La reutilización de la información sanitaria desde la perspectiva de la regulación europea sobre gobernanza de datos. Andreu Martínez, B. (dir.), *Los datos de salud como eje de la transformación digital de la Sanidad.* Comares, Granada. pp. 45-68.

21 Cfr., Reglamento (UE) 2025/327 del Parlamento y del Consejo de 11 de febrero de 2025 relativo al Espacio Europeo de Datos de Salud, y por el que se modifican la Directiva 2011/24/UE y el Reglamento (UE) 2024/2847. DOUE L 327, de 5.3.2025.

22 DOUE L 2518, de 12.12.2025.

23 El Comité Europeo de Protección de Datos (CEPD), del que forman parte todas las autoridades independientes de protección de datos -o, en inglés *European Data Protection Board* (EDPB)- y el Supervisor Europeo de Protección de Datos (SEPD) emitieron el Dictamen conjunto el 10 de febrero de 2026, cfr., EDPB-EDPS JOINT OPINION 2/2026, *On the Proposal for a Regulation as regards the simplification of the digital legislative framework (Digital Omnibus)*, adoptado el 10 de febrero de 2026. Disponible en: https://www.edpb.europa.

documento, declaran su oposición a la propuesta de limitación de la definición de "datos personales", asimismo, expresan su inquietud ante las reformas normativas propuestas que afectan a cuestiones clave del RGPD y de la Directiva ePrivacy[24], según lo planteado en el "Ómnibus Digital" por la Comisión Europea. La consulta detallada de dicho texto resulta muy recomendable, observando las acertadas consideraciones ofrecidas. Pues, además, se muestran varias dudas sobre otros aspectos propuestos, estimando que no es necesario restringir los derechos reconocidos, tampoco modificar cuestiones que ya están reguladas de forma clara. Entre otras, también se cita que no es procedente alterar las bases jurídicas fijadas en lo relativo a la IA, ni las restricciones al derecho de acceso. Con todo, como bien se indica cabe insistir en primar la transparencia informativa.

En cualquier caso, sirva lo apuntado para mostrar el interés que despierta la actual reforma impulsada desde la Comisión Europea, así como la valoración crítica que ha sido referenciada al respecto. A su vez, como reconocimiento del valor de los actuales textos legales vigentes en la UE, como ha sido expuesto en este epígrafe del trabajo. No parece esencial ni oportuno proceder ahora a reformar normativas que son nítidas y ofrecen seguridad jurídica, como bien ha declarado el Dictamen precitado.

3. El nuevo "paquete normativo Ómnibus digital": objetivos y principales características del nuevo enfoque regulatorio.

Como ha sido avanzado, la Comisión Europea presentó el 19 de noviembre de 2025 el "paquete ómnibus digital"[25], cuyo objetivo es proceder a la revisión y modificación de la normativa vigente, con la finalidad de simplificar determinadas cuestiones. En especial, en materia de datos, inteligencia artificial y ciberseguridad y datos (personales y no personales). En este apartado son identificados sus principales objetivos y novedades. Si bien, en estos momentos, queda esperar a su tramitación legislativa, vía el procedimiento ordinario, conforme a lo previsto, para que las propuestas normativas formuladas puedan ser debatidas tanto en el Parlamento Europeo como en el Consejo, y, en su caso, pudieran ser presentadas enmiendas. Todo ello, por tanto, está en curso y convendrá estar atentos, hasta conocer el acuerdo sobre el texto legal definitivo que sea adoptado.

En concreto, el citado paquete normativo que ha sido propuesto por la Comisión está integrado por dos propuestas de Reglamento (UE), a saber,

(A) la Propuesta de Reglamento del Parlamento Europeo y del Consejo que modifica los Reglamentos (UE) 2016/679, (UE) 2018/1724, (UE) 2018/1725, (UE) 2023/2854 y las Directivas 2002/58/CE, (UE) 2022/2555 y (UE) 2022/2557 para la simplificación del marco legislativo digital y que deroga los Reglamentos (UE) 2018/1807, (UE) 2019/1150, (UE) 2022/868, y la Directiva (UE) 2019/1024. El objetivo de esta propuesta radica en la reforma y actualización de varias normativas, a saber, el RGPD, la Directiva 2002/58/CE, el Reglamento (UE) 2023/2854 sobre normas armonizadas para un acceso justo a los datos y su utilización (el "Reglamento de Datos"), la Directiva 2022/2555 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión ("Directiva NIS2") y otras normas relacionadas con el uso de datos. Y,

(B) la Propuesta de Reglamento del Parlamento Europeo y del Consejo por la que se modifica los Reglamentos (UE) 2024/1689 por el que se establecen normas armonizadas en materia de IA ("Reglamento de IA") y (UE) 2018/1139 para la simplificación en la implementación de normas armonizadas en materia de inteligencia artificial, siendo objetivo principal de esta última, en síntesis, la modificación de determinados aspectos previstos por el actual Reglamento (UE) 2024/1689 ("Reglamento de IA")[26]. Con ello, se pretende promover su progresiva aplicación, para que resulte más eficaz y eficiente.

De este modo, en puridad, serían reducidas las cargas legales a los sujetos obligados y, por ende, los costes, en especial, por lo que respecta a pequeñas o medianas empresas (pymes), o aquellas sociedades mercantiles calificadas como *small mid-caps* o *mid-caps*. A su vez, es de interés colectivo reforzar las medidas preventivas y la seguridad jurídica.

Por tanto, en el supuesto de que fueran aprobadas estas propuestas -sin modificaciones o, en su caso, en atención a los textos definitivos que fueran adoptados-, lo cierto es que sí se muestra una nueva orientación legislativa. Podría tener lugar una reforma

eu/system/files/2026-02/edpb_edps_jointopinion_202602_digitalomnibus_en.pdf

[24] Vid. la conocida como Directiva europea de *ePrivacy*, Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio de 2002 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas). DOUE L 201, de 31.7.2002. Esta normativa regula de forma específica lo relativo a la privacidad y protección de las comunicaciones electrónicas. También, se establece el régimen aplicable al posible empleo de *cookies* y análogas técnicas de seguimiento en la red o el entorno digital. Asimismo, completando lo regulado en esta materia, el Reglamento (UE) 2021/1232 del Parlamento Europeo y del Consejo de 14 de julio de 2021 por el que se establece una excepción temporal a determinadas disposiciones de la Directiva 2002/58/CE en lo que respecta al uso de tecnologías por proveedores de servicios de comunicaciones interpersonales independientes de la numeración para el tratamiento de datos personales y de otro tipo con fines de lucha contra los abusos sexuales de menores en línea (DOUE L 274, de 30.7.2021).

[25] Cfr., Propuesta de Reglamento del Parlamento y del Consejo por el que se modifican los Reglamentos (UE) 2024/1689 y (UE) 2018/1139 en lo que respecta a la simplificación de la aplicación de las normas armonizadas sobre inteligencia artificial (Ley Omnibus Digital sobre IA). Bruselas, 19.11.2025. COM(2025) 836 final.

[26] Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo de 13 de junio de 2024 por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) nº. 300/2008, (UE) nº. 167/2013, (UE) nº. 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial). DOUE L 1689, de 12.7.2024.

muy significativa que afectaría a textos legales europeos que son hoy fundamentales. Por consiguiente, conlleva un cambio radical en las bases regulatorias que han de regir el derecho digital, la protección y el tratamiento de los datos, y, además, de forma extensiva, la gobernanza del dato. Toda vez que serían objeto de revisión, modificación o actualización varias normas -como ha sido reseñado con carácter previo en este trabajo-: el RGPD, el Reglamento europeo de IA y el Reglamento europeo de Datos.

Con todo, según cabe interpretar a la luz de los objetivos y cambios propuestos, la principal pretensión europea, ahora, se centra en tratar de adecuar o adaptar el Ordenamiento vigente a las oportunidades o posibilidades que ofrece el desarrollo de la IA. Ello, a su vez, se infiere de lo manifestado con carácter previo en el texto de la Comunicación de la Comisión Europea al Parlamento Europeo y al Consejo: *Estrategia para una unión de datos- Desbloqueo de datos para la IA*, de 19.11.2025[27]. Por lo cual, el nuevo enfoque normativo que ha sido propuesto no resulta algo sorprendente, pues era esperado.

En este momento, no se puede ignorar que se abre un frente complejo, muy sensible en lo técnico y jurídico. Los desafíos que se plantean son relevantes, siendo pragmáticos, por lo que concierne al Derecho y, en particular, a la posible reconfiguración de criterios o reglas, así como en lo relativo a los derechos y garantías. Así se estima, ante la prevista reforma del Reglamento General de Protección de Datos (RGPD)[28], entre otras medidas. Si bien, en principio, estas innovaciones responderían -según se infiere- al buen propósito europeo de simplificación administrativa y, a su vez, de facilitar el desarrollo de la inteligencia artificial (IA). No obstante, lo cierto es que sí se podría provocar importantes distorsiones o cambios disruptivos en el actual modelo regulatorio.

De igual modo, nótese que ya ha sido adoptado, a fecha actual y dentro del primer paquete o conjunto de normas que desarrollan el actual texto del RGPD, el Reglamento (UE) 2025/2518 del Parlamento Europeo y del Consejo, de 26 de noviembre de 2025, por el que se establecen normas procedimentales adicionales sobre la garantía del cumplimiento del Reglamento (UE) 2016/679[29]. Con este reciente nuevo Reglamento europeo se trata de dotar de mayor eficacia al RGPD, estableciendo medidas que permitan optimizar el procedimiento aplicable y, de forma específica, asegurar la mejora de los procesos internos de las entidades que operan en la UE, así como la acción coordinada y más eficaz de las autoridades competentes. A dicho fin, en el mismo, ya están previstas medidas de simplificación administrativa, para incrementar la agilidad de los procedimientos en caso de reclamaciones transfronterizas y que estas pudieran ser resueltas de forma adecuada. Además, se obliga a las correspondientes autoridades de protección de datos de cada Estado miembro a cooperar con objeto de ofrecer tutela más eficiente, evitando demoras injustificadas.

Por lo cual, queda patente que con esta última normativa aprobada han sido aportadas mejoras aplicativas o procedimentales. Pero, más allá de lo señalado, con las nuevas propuestas normativas del Ómnibus Digital, se abre la puerta a otras innovaciones más sustanciales, con mayor relieve e impacto. Estas implicarían notables transformaciones legales, siendo radicales en algunos aspectos, como ha sido apuntado con carácter previo. Entre otras, cabe reseñar la posible redefinición "a la carta" de la noción legal de "dato personal" o "datos personales". Toda vez que, frente al concepto genuino acuñado por el RGPD (artículo 4.1.), ahora, se lo podría instrumentalizar a los únicos fines del mercado digital o la implementación de la IA. O dicho de otro modo, se orientaría una mayor flexibilidad interpretativa del mismo, no justificada y que podría afectar al derecho de protección que le había sido otorgado en origen por el RGPD de 2016. De igual modo, se observa con la modificación prevista por el Ómnibus Digital en lo relativo a algunos de los deberes de tratamiento de los datos que corresponden a los responsables de datos, al suprimir ciertas obligaciones o su eventual grado de exigibilidad o en ciertos supuestos, por ej., en el caso de pequeñas o medianas empresas. Lo advertido, en la práctica, puede conllevar el debilitamiento de la protección de datos y, por ende, generar riesgos añadidos. Por lo cual, no parece justificado.

Lo apuntado bien ilustra sobre el renovado enfoque que ha sido impulsado o se promueve. Con lo cual, en la actualidad, surge de nuevo el debate jurídico sobre la necesidad de reforzar el alcance del derecho a la protección de los datos y la protección de los intereses legítimos que pudieran quedar afectados frente a la implementación extensiva de las tecnologías emergentes como la IA[30].

En todo caso, con motivo de las nuevas reformas regulatorias planteadas por la Comisión, resulta de interés consultar el Dictamen conjunto que ha sido emitido por el Comité Europeo de Protección de Datos (CEPD) y el Supervisor Europeo de Protección de Datos (SEPD) sobre las propuestas de Reglamentos presentadas[31], modificando varias

---

27 Comunicación de la Comisión Europea al Parlamento Europeo y al Consejo: *Estrategia para una unión de datos-Desbloqueo de datos para la IA*. Bruselas, 19.11.2025, COM/2025/835 final, en: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52025DC0835 Asimismo, más informae ción al respecto, en: https://spain.representation.ec.europa.eu/noticias-eventos/noticias-0/la-simplificacion-de-normas-digitales-y-las-nuevas-carteras-digitales-permitiran-ahorrar-e-impulsar-2025-11-19_es

28 Cfr., Comisión Europea: "*Propuesta de Reglamento Omnibus Digital sobre la IA"*, Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se modifican los Reglamentos (UE) 2024/1689 y (UE) 2018/1139 en lo que respecta a la simplificación de la aplicación de normas armonizadas en materia de inteligencia artificial (Reglamento ómnibus digital sobre IA). COM (2025) 836 final, 2025/0359(COD). Bruselas, 19.11.2025.

29 DO L 2518 de 12.12.2025.

30 Al respecto, vid., Guasch Portas, V. y Soler Fuensanta, J.R. (2015): El interés legítimo en la protección de datos. RDUNED, *Revista de Derecho UNED*, 16, pp. 417-438. Disponible en: https://revistas.uned.es/index.php/RDUNED/article/view/15245 (Fecha consulta: 10/02/2026). González Mendoza, D.P. (2024): *El alcance del derecho a la protección de datos personales en las administraciones públicas*. Aranzadi, Cizur Menor.

31 Cfr., Dictamen conjunto emitido por el Comité Europeo de Protección de Datos (CEPD) y el Supervisor Europeo de Protección de Datos (SEPD) sobre la propuesta de Reglamento de la Comisión Europea por el que se modifican determinados Reglamentos UE: *EDPB-EDPS Joint Opinion 01/2025 on the Proposal for a Regulation on simplification measures for SMEs and SMCs, in particular the record-keeping obligation*

Leyes UE -como hemos referenciado- y también, en concreto, el RGPD. En dicho documento, se examina la reforma anunciada en mayo de 2025, así como las medidas encaminadas a simplificar el deber de llevar un registro de actividades de tratamiento por parte de los sujetos responsables del mismo (artículo 30 del RGPD) y, de igual modo, lo relativo a la posibilidad de facilitar el cumplimiento de otras obligaciones cuando se tratara de pymes o de empresas calificadas como "*small mid-cap enterprises*" (SMC).

3.1. Principales objetivos

Los principales objetivos de la propuesta se centran en una finalidad estratégica que no pasa inadvertida; esta es, promover el desarrollo de la IA, su empleo aplicativo en los distintos ámbitos o sectores, como ha sido advertido. El interés que concurre o, en su defecto, sería subyacente parece claro -en nuestra opinión-, toda vez que se pretende la revisión de varias normativas consolidadas e introducir nuevas medidas destinadas a la simplificación en los deberes relativos al tratamiento del dato. Así como otras, orientadas a dinamizar el emprendimiento tecnológico mediante la incorporación acelerada de sistemas basados en IA. De ahí que, en especial, se pongan en el punto de mira aquellos aspectos que pudieran facilitar la oportuna implementación de este tipo de herramientas. Y una vez identificados, a dicho fin, se procede a "remodelar" las reglas inicialmente previstas en el vigente Reglamento europeo de IA (2024). Esto es, con el propósito de paliar la complejidad de lo ya preceptuado, son objeto de revisión sus preceptos y, en particular, aquellos criterios y medidas que por su alto o mayor nivel de exigencia pudieran plantear mayor dificultad o cargas legales para el desarrollo de la IA en la UE.

De este modo, en síntesis, cabe interpretar la propuesta de modificación planteada conforme al siguiente enunciado: reducir, en la medida posible, los aspectos normativos que pudieran suponer una limitación u obstaculizar la efectiva implementación de la IA.

A la vista de la propuesta Ómnibus Digital, cabe significar que con las reformas propuestas se hace hincapié especial en cuatro cuestiones, las cuales, a su vez, se configurarían como objetivos principales. Estas son: (a) mitigar la complejidad regulatoria; (b) simplificación administrativa y reducción de las cargas económicas que conlleva el deber de cumplimiento legal de las obligaciones. Esto supone, en suma, reducir los costes que las entidades han de asumir para asegurarse de cumplir con la normativa que rige el mercado digital. Lo señalado, en principio, podría estimarse como favorable para promover el emprendimiento innovador o tecnológico, al tratarse de medidas que fueran destinadas a pymes europeas o de mediana capitalización (con menos de 750 empleados y con un volumen de negocio anual que no supere los 150 millones de euros, o bien que su balance general no supere la cifra de 129 millones de euros). También otro objetivo es (c) optimizar la competitividad de las empresas; (d) fomentar la innovación, el desarrollo y el emprendimiento tecnológico, así como impulsar al sector digital europeo. Pero, para que pudiera ser mejor valorado, aún es preciso que estas medidas proyectadas pudieran ser más concretadas por el legislador europeo.

No obstante, a nuestro juicio, se deberá garantizar -en cualquier caso- un nivel de observancia satisfactorio por lo que respecta al Ordenamiento vigente. En particular, en lo relativo a la calidad y la obligación de no vulnerar los derechos fundamentales reconocidos como son, entre otros, la protección de datos, la privacidad y la seguridad. Con todo, a dichos efectos, es y será esencial, insistir en el deber de tutela y en el desempeño de las funciones de control o supervisión, tanto por parte de las autoridades competentes nacionales como europeas, actuando de forma coordinada y colaborativa.

3.2. Principales reformas regulatorias

Las modificaciones normativas propuestas por la Comisión Europea, en concreto, gravitan en torno a seis cuestiones principales. Estas son identificadas a continuación:

(i) *Promover el emprendimiento innovador y tecnológico basado en sistemas de IA*. A dicha finalidad, desde la Comisión europea se propone la reforma del actual Reglamento europeo de IA (RIA, en adelante) en determinados aspectos. Ello, con objeto de facilitar que las empresas, en especial, las pymes, pudieran reducir su carga de cumplimiento legal y, por ende, el coste económico que supone, para optimizar sus resultados y, de este modo, afrontar con éxito los desafíos competitivos que en este terreno se plantean.

La simplificación administrativa puede ser en tal sentido una medida favorable, en particular, para las entidades que sean pequeñas empresas o de mediana capitalización. No obstante, reducir los requerimientos exigidos por lo que respecta a la documentación técnica y procedimientos de acreditación es una de las medidas más debatidas.

Asimismo, se trata de incrementar el ámbito subjetivo de la norma, de manera que existan más posibilidades participativas. En este sentido, en orden al desarrollo de la IA aplicativa, se propone que un mayor número de empresas u operadores puedan acceder a los denominados "entornos controlados de pruebas" (*sandboxes*) o los calificados con la expresión "*sandboxes* regulatorios". Con ello, se optimizan recursos y seguridad, ya que la IA es aplicada en espacios seguros y supervisados, donde las empresas y desarrolladores podrían realizar prácticas o pruebas experimentales, antes de proceder a la validación de sistemas o modelos. Estas acciones resultan convenientes, siempre con carácter previo a la efectiva implementación de las oportunas herramientas de IA. En todo caso, el proceso de verificación es preciso antes de cualquier tipo de uso o destino comercial. La dinámica del *sandbox*

under Art. 30(5) GDPR, adoptado el 8 de julio de 2025, en: https://www.edpb.europa.eu/system/files/2025-07/edpb_edps_jointopinion_202501_proposalsimplification_en.pdf

permite la actuación colaborativa entre distintos agentes, por ejemplo, sujetos usuarios y proveedores de IA. A su vez, aproxima la comunicación y cooperación activa con las autoridades competentes y las posibles entidades desarrolladoras de IA, colaborando en la determinación de buenas prácticas y guiando su satisfactoria implementación.

Por otra parte, entre otras medidas, se propone reforzar las competencias de la Oficina Europea de IA[32] y en orden a centralizar las funciones de supervisión de los sistemas de IA o basados en distintos modelos de IA. El papel que compete a la misma se estima principal, por lo cual se propone reforzar sus funciones. Todo ello, además, tendría como finalidad común asegurar una eficaz aplicación del RIA.

(ii) *Racionalización administrativa*, y centralización de los servicios prestados por lo que respecta a la constitución de una única ventanilla para la comunicación o notificación de incidencias en materia de seguridad. Ello, de igual modo, contribuirá a la simplificación y mayor agilidad de los procedimientos, conforme a lo previsto por la normativa digital UE, en concreto, según lo preceptuado por el RGPD y por la Directiva NIS2 (Directiva UE 2022/2555 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en la Unión)[33]. En virtud de las precitadas, hasta ahora, se establecen obligaciones específicas de notificación de los posibles incidentes adversos que pudieran producirse en diferentes organismos. De esta forma, se trata de facilitar su cumplimiento vía una única comunicación. Ello, por tanto, conllevaría la centralización del servicio y del canal de comunicación, a su vez, asegurando la adecuada coordinación administrativa en las actuaciones de respuesta.

(iii) *Configuración de un ámbito de privacidad apropiado para el emprendimiento innovador*. A dichos efectos, se propone por la Comisión la revisión de lo preceptuado por el RGPD, con objeto de incorporar medidas específicas que contribuyan a este objetivo, entre otras, en materia de tratamiento de datos personales. Por ejemplo, admitir como posible interés legítimo, alegado como base de legitimación o justificación, el empleo de este tipo de datos en lo relativo al desarrollo operativo de la IA, así como para su proceso de entrenamiento. Incluso, el eventual uso de estos datos mediante aplicaciones de biometría (datos biométricos)[34]. En concreto, esta técnica requiere la captación, empleo o registro de datos personales para operar, como -por ejemplo- a través de la obtención de imágenes que se centran en rasgos identificativos. Y como tales, aspectos que son propios de cada individuo, intrínsecos o inalterables de la persona. Con ello, se pueden trazar perfiles o plantillas biométricas, siendo a su vez empleados para diferentes fines, como medios de identificación, autenticación, localización en espacios, entre otros factibles.

La posible implementación de este tipo de tecnologías analíticas o sistemas que posibilitan exámenes basados en biometría también conlleva cierta problemática e incrementa los riesgos, pues, en algunos casos. se pudieran vulnerar derechos o resultar muy intrusiva[35]. Así, por ejemplo, cabe pensar, cuando se utilizaran determinadas técnicas analíticas o biométricas aplicando sistemas basados en IA, entre otras posibilidades.

Por consiguiente, estas propuestas suscitan importantes controversias. Aun cuando quedara previsto o se habilitara la posibilidad de estas acciones, han de ser realizadas con el previo consentimiento de los interesados, o, en su defecto, informando con carácter previo al afectado. Pues, con todo, se trata de un tema sensible, dado que afecta a derechos fundamentales, protección de datos y privacidad.

(iv) *Reducción de las obligaciones que corresponden a los responsables del tratamiento de datos personales*. Otra de las modificaciones planteadas en materia de tratamiento de datos personales podría suponer reducir

---

32 La Oficina de IA desempeña sus funciones en colaboración con el Comité Europeo de Inteligencia Artificial, integrado por los representantes de los Estados miembros, y el Centro Europeo para la Transparencia Algorítmica (ECAT) de la Comisión Europea. Información al respecto, en: https://digital-strategy.ec.europa.eu/es/policies/ai-office (Fecha consulta: 15/03/2026).

33 Cfr., 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, por la que se modifican el Reglamento (UE) nº. 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2). *DOUE L 333, de 27.12.2022.* Con relación a la Directiva **NIS2** y en materia de ciberseguridad, cfr., la información práctica aportada por INCIBE, "NIS2: lo que necesitas saber", en: https://www.incibe.es/incibe-cert/sectores-estrategicos/NIS2-necesitas-saber (Fecha consulta: 14/03/2026).

34 Acerca de las posibilidades que ofrece la biometría, como técnica aplicable que posibilita exámenes basados en biometría, véase, entre otros, Menéndez González, N. (2024): Retos para la protección de datos en el uso de tecnologías de reconocimiento facial, en Pérez Díaz, R.; González Mendoza, D. P. y Vega García, P., *Perspectivas Transversales del Derecho a la Protección de Datos Personales*. Colex, A Coruña (pp. 131-143). Razquin Lizarraga, M.M. (2024): Notas sobre el Dictamen 11/2024 del CEPD sobre uso del reconocimiento facial en el flujo de pasajeros en aeropuertos a la luz del Reglamento de Inteligencia Artificial y del RGPD", *Derecho Digital e Innovación*, 20. Romeo Casabona, C.M. (2021): Datos biométricos (Comentario al artículo 4.14 RGPD), en Troncoso Reigada, A. (Dir.), *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos Personales y Garantía de los derechos digitales.* Thomson Reuters Aranzadi, Cizur Menor (Vol. I, pp. 709-714). Asimismo, el trabajo de González Mendoza, D.P. (2025): Los datos biométricos y las tecnologías que los utilizan para su funcionamiento: Régimen jurídico aplicable y potenciales riesgos. *Revista Vasca de Administración Pública* (RVAP), 132, pp. 427-464.

35 Vid., INCIBE, "Tecnologías disruptivas para la empresa segura. Instituto Nacional de Ciberseguridad", 2020, https://www.incibe.es/empresas/blog/tecnologias-disruptivas-empresa-segura. (Fecha consulta: 20/02/2026).

algunos de los deberes que, de acuerdo con lo exigido por el texto legal vigente del actual RGPD, corresponden a los responsables de datos en las empresas/pymes. Entre estas obligaciones, se suprimiría la relativa al registro de actividades o medidas de tratamiento o en determinados supuestos.

Obsérvese que, de forma expresa, en el actual RGPD se define la figura del sujeto responsable o los responsables del tratamiento de datos en el artículo 4, apartado 7 del RGPD, como *la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento* (...). Por lo tanto, es el sujeto o entidad la que decidirá sobre los fines y los medios empleados y, como tal, se le atribuye el deber principal de cumplir con la normativa vigente, proteger los datos y garantizar el ejercicio de los derechos de los interesados[36].

Además, de acuerdo con el vigente RGPD, entre las obligaciones establecidas y que de forma clara corresponden a los sujetos u operadores responsables del tratamiento de datos[37], cabe destacar: (1) La incorporación necesaria de la figura del *delegado de protección de datos* (DPD). El RGPD obliga a quienes realicen ciertos tratamientos a designar un delegado, que ha de ser un profesional experto, que disponga de una formación específica y acreditada, tanto en protección de datos como en análisis de riesgos y medidas de seguridad de la información. Podrá ser personal interno o externo a la entidad u organismo. (2) El *deber de registrar documentalmente las acciones y procesos de tratamiento*, que corresponde tanto a los responsables de ficheros -de forma principal- como a los posibles encargados del tratamiento de datos. Estas figuras son definidas en el artículo 4, apartados 7 y 8. (3) El deber de información previa o inmediata a los interesados o al interesado. Y, en ciertos casos, exige "disponer de su previo consentimiento expreso". En consecuencia, al respecto, no sería suficiente con un consentimiento tácito, por lo que las empresas u operadores quedan obligados a solicitar dicho consentimiento, en tiempo y forma adecuada, asegurando la debida aceptación expresa y constancia de la misma. (4) El deber de información, en todo caso, ha de ser cumplido de forma adecuada por todo tipo de entidad u organización, reforzando la transparencia informativa. (5) Es necesario implementar métodos de *evaluación de impacto y análisis de riesgos,* haciendo especial referencia al tratamiento de cierta tipología de datos, medidas preventivas y de seguridad adoptadas. (6) Se establece la obligación de notificar cualquier clase de incidencia o vulneración de los sistemas de seguridad implementados relativos a los datos personales. Así, en el plazo máximo de 72 horas deberá ser comunicada cualquier eventualidad a la Agencia Española de Protección de Datos (AEPD) y, de igual modo, en casos graves será necesario notificarlo a los afectados o interesados, con el fin de evitar mayores daños o perjuicios. Por último, (7) se exige a la entidad u operador la plena adecuación de los modelos contractuales empleados a esta normativa.

En todo caso, a nuestro juicio, conforme a lo preceptuado en el RGPD, cabe hacer mayor hincapié en el principio de responsabilidad proactiva o principio de *accountability*. Toda vez que ha de ser la máxima a seguir, en todos los ámbitos y sectores, privado y público. También, de igual modo, por lo que respecta a las Administraciones y resto de entidades que integran el sector público, ya que están llamadas a ilustrar con su ejemplo de buena gestión y actuación responsable.

Este principio, en concreto, se establece en el artículo 5.2 del RGPD**,** obligando a todos los responsables del tratamiento de los datos- a actuar con la debida diligencia. Esto es, adoptando las medidas necesarias y cumpliendo con las obligaciones impuestas por la normativa. A su vez, lo señalado ha de poder ser verificado, acreditando su efectividad. Con lo cual, comprende realizar varias actuaciones, entre otras, aquellas previas relativas a la evaluación del impacto y la gestión del riesgo y, en consecuencia, adoptar las medidas preventivas oportunas[38].

De todo ello ha de tenerse constancia y documentarlo, pues, solo de este modo podría ser viable su acreditación o prueba. Ha de poder ser demostrado su cumplimiento efectivo, junto a los otros requerimientos fijados en el artículo 5 del RGPD. De esta forma, se configuran los siete principios básicos y rectores aplicables al tratamiento de datos personales: (1) Licitud, transparencia y lealtad. (2) Limitación de la finalidad. (3) Minimización de datos. (4) Exactitud. (5) Limitación del plazo de conservación. (6)

[36] Sobre las obligaciones que corresponden a todo responsable del tratamiento de datos, conforme al actual RGPD, vid., AEPD, "Guía del Reglamento General de Protección de Datos para responsables de tratamiento". Madrid 2018. Disponible en: https://www.aepd.es/media/guias/guia-rgpd-para-responsables-de-tratamiento.pdf (Fecha última consulta: 20/02/2026).

[37] Al respecto, resulta de interés examinar el articulado del vigente RGPD y, a su vez, en relación con el texto de la legislación española que lo complementa en nuestro Ordenamiento nacional, dictada de acuerdo con el mismo. Para mayor detalle, vid., López Calvo, J., coord. (2019): *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPD-GDD*. Wolters Kluwer España, Madrid.

[38] Para mayor detalle sobre estos aspectos principales, vid., AEPD, "Gestión del riesgo y evaluación de impacto en tratamientos de datos personales", 29 de junio de 2021. Disponible en: https://www.aepd.es/guias/gestion-riesgo-y-evaluacion-impacto-en-tratamientos-datos-personales.pdf. AEPD, "Guía de Protección de Datos por defecto", 8 de octubre de 2020. https://www.aepd.es/guias/guia-proteccion-datos-por-defecto.pdf (Fecha consultas: 10/02/2026).

Integridad y confidencialidad (seguridad de los datos). (7) Principio de responsabilidad proactiva o responsabilidad acreditada[39].

(v) *Actualización del régimen aplicable a las cookies*. Se trata de modificar la frecuencia de su comunicación a los usuarios, de forma que se facilitaría la posibilidad de otorgar un único consentimiento con efecto amplio o extensivo. Esto es, en la práctica, podría servir con pulsar un solo "clic" de aceptación. Este punto, de igual modo, plantea dudas, por cuanto esta reforma propuesta podría afectar al deber de aportar información detallada al interesado y, en todo caso, con carácter previo a cualquier tipo de posible aceptación por su parte. Por ende, generaría un déficit de confianza y, desde luego, la falta de la necesaria transparencia informativa. Por tanto, no parece razonable, incluso, aunque los usuarios pudieran configurar sus preferencias seleccionadas y gestionarlas en su navegador.

(vi) *Optimizar la accesibilidad y la disponibilidad de los datos*. La Comisión propone medidas para armonizar la normativa europea relativa al acceso, empleo y reutilización de datos, tanto en el caso de los datos de carácter personal -o datos personales- como aquellos que no lo fueran -datos no personales-. Los datos dinámicos son un activo muy apreciado, como ha sido expuesto a lo largo de este trabajo, por ende, pretende simplificar la regulación para procurar facilitar su grado de cumplimiento.

A dicho fin, se hace hincapié en el Reglamento (UE) de Datos o *Data Act* (2023), previa revisión o modificación de las otras normativas actuales que quedarían afectadas, tal y como se infiere a la luz de lo planteado por la Comisión Europea. En consecuencia, las implicaciones de esta propuesta son relevantes también al incidir, de forma principal, en el RGPD (2016), la Directiva (2019) relativa a los datos abiertos y la reutilización de la información del sector público[40], y el Reglamento de Gobernanza de datos (2022), entre otras principales normas europeas. Toda vez que parece plantearse la unificación de estos regímenes jurídicos o cuerpos legales específicos en torno a un único bloque legal: el mencionado Reglamento (UE) de datos o *Data Act*. Con lo cual, cabe interpretar que este, a su vez, sería reformado para servir de nueva cobertura legal, a modo de paraguas normativo único en materia de gestión o gobierno de datos.

En cualquier caso, sobre esta proyectada unificación normativa surgen varios interrogantes, siendo preciso que sea ofrecida mayor concreción o detalle por parte del legislador. Pues, además, con ocasión de esta reforma, se tratarían de incorporar más exenciones legales o excepciones *ad hoc* en lo relativo a los deberes impuestos -en la actualidad- a los proveedores de servicios o, en su caso, en supuestos de cambios de proveedor de servicios en la nube. Asimismo, implicaría la revisión de los modelos contractuales, estableciendo nuevas cláusulas o condicionamientos. También, por otra parte, lo mencionado podría conllevar el obligatorio desbloqueo de datos protegidos, para su configuración como datos abiertos u *open access*.

De este modo, en suma, se pretende que la apertura y la disponibilidad de los datos -de todo tipo- sea máxima. Con lo cual, afectaría a todo tipo de conjuntos de datos, dinámicos y de calidad, en especial, aquellos que presentaran mayor valor o alto interés.

Con todo, como resulta patente, lo propuesto por la Comisión en este sentido es buena muestra y sirve de resumen de lo ya advertido *supra*: las reformas propuestas son enfocadas, de forma principal, hacia el desarrollo de la IA.

El nuevo enfoque, por ende, implica un cambio radical en la orientación de la regulación europea en materia de protección y tratamiento de los datos, dando paso a un nuevo régimen centrado en la utilidad instrumental de la IA, facilitando su entrenamiento e incorporación aplicativa de forma extensiva. Este sería, en suma, el interés prioritario que subyace como motivación del nuevo paquete normativo. Por tanto, en puridad, se iría más allá de cualquier otra pretensión promotora o de simplificación normativa y administrativa, como ha sido anunciado inicialmente.

4. Consideraciones de especial relevancia desde la óptica del Derecho administrativo y en atención al contexto digital con la incorporación de la IA.

Como ha sido señalado, la precitada Estrategia Europea de Datos orienta sus medidas de acción hacia la configuración del "mercado único (digital) de datos" que la UE pretende liderar. Por lo cual, los datos son el elemento básico sobre el que gira lo programado y en atención a los objetivos declarados[41]. A su vez, en dicho entorno digitalizado y con alta proyección económica, como se sabe, es posible la libre circulación y disponibilidad de distintos tipos de información, documentos o datos.

Dicha programación se justificaría -según se argumenta desde la UE- en interés general o público, aludiendo a las posibles ventajas o beneficios colectivos que se aportarían con ello. De esta forma, parece ser que -en principio- los efectos positivos que

39 En este sentido, KPMG: "RGPD y las claves de la responsabilidad proactiva para su aplicación", 18 mayo 2023, https://www.tendencias.kpmg.es/2023/05/rgpd-claves-responsabilidad-proactiva-aplicacion/ (Fecha consulta:11/02/2026).

40 Directiva (UE) 2019/1024 del Parlamento Europeo y del Consejo de 20 de junio de 2019 relativa a los datos abiertos y la reutilización de la información del sector público. DOUE L 172, de 26.6.2019. Y, en concreto, en materia de datos abiertos y reutilización de datos, aportando un completo análisis de la norma, vid., los estudios realizados por los autores que integran la *op. col.,* Julián Valero Torrijos, J. y Martínez Gutiérrez, R., dirs. (2022): *Datos abiertos y reutilización de la información del sector público*. Comares, Granada.

41 Cfr., Comisión Europea: Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a un mercado único de servicios digitales (Ley de servicios digitales) y por el que se modifica la Directiva 2000/31/CE. COM/2020/825 final. Bruselas, 15 diciembre 2020. https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=COM:2020:825:FIN.

pudieran generarse repercutirían tanto en el sector privado como público. No obstante, lo cierto es que lo señalado quedaría por verificar en la práctica, evaluando los resultados obtenidos y, a su vez, analizando costes/riesgos y beneficios.

En cualquier caso, más allá de lo pretendido por la UE o esperado, deberá observarse la posible concurrencia de varios factores -como ha sido apuntado con carácter previo- y, desde luego, para alcanzar los objetivos estratégicos sería esencial lograr una efectiva coordinación, cooperación y colaboración entre sectores público/privado en la UE.

De igual modo, en este contexto y en atención a los objetivos estratégicos previstos, consideramos que es necesario examinar otras cuestiones esenciales, como son -por ejemplo- la de vigilar con eficacia las prácticas que los operadores puedan ejecutar y conforme a la legalidad vigente. En consecuencia, estimamos que cabe hacer mayor hincapié en las actividades específicas de control o supervisión por parte de las autoridades competentes, con objeto de vigilar de forma efectiva que se presten servicios digitales seguros y prácticas responsables, conforme a las reglas de la competencia. Pues, con todo, la observancia del cumplimiento legal ha de ser fundamental. También, convendrá reforzar los medios destinados a la protección de los consumidores o usuarios y, en general, de los ciudadanos. Asimismo, se deberá resolver la brecha digital, problema que aún se pone de manifiesto[42].

Cabe entender que todo ello resultará esencial para procurar la buena marcha de la economía de los datos, como se plantea o pretende desde la UE, y evitando riesgos, sobre todo, si realmente se trata de actuar en interés colectivo o, en especial, de la ciudadanía. Por ende, a dicho fin, se deberán habilitar recursos y aportar máximas garantías jurídicas. En este sentido, consideramos que ahora recobra importancia poder ofrecer una protección eficaz a los derechos e intereses legítimos de los ciudadanos, en especial, por lo que corresponde al posible uso de (sus) datos. Además de los eventuales riesgos adicionales que puede suponer la incorporación de herramientas de IA.

En definitiva, cabe pensar que para alcanzar los objetivos de esta Estrategia es necesario, ante todo, contar con un adecuado marco regulatorio, eficaz y aplicable de forma común, fijando criterios claros y uniformes para poder asegurar una "buena gobernanza de los datos*"*. Este es, sin duda, el punto de partida fundamental, pero, todavía queda por evaluar su ejercicio y efectos. Pues, si bien la UE quiere ser líder en este ámbito, de acuerdo con la pretensión manifestada al configurar "un modelo de sociedad empoderada por los datos" y a través del proyectado *mercado único de datos*, sería necesario aún prevenir varias cuestiones, como ha sido expuesto. Así, según se apunta por la UE, este mercado posibilitaría "desbloquear los datos no utilizados" de forma que pudieran circular libremente entre sectores y proporcionar beneficios colectivos a empresas, investigadores y administraciones públicas[43]. De este modo, lo cierto es que la denominada "economía de los datos" ligada al mercado digital se centra, como principal meta, en el actual escenario estratégico trazado desde la UE. Y al servicio de dicho objetivo, se pretende facilitar los oportunos medios. Conforme con este planteamiento, los datos, en consecuencia, serían el recurso clave al servicio de dicho fin.

Por tanto, queda patente que disponer de una regulación armonizada en la UE en esta materia es y será fundamental. Esta cuestión, de forma especial, debe ser analizada desde el Derecho Administrativo, pues, en este terreno -como ha sido señalado *supra*-, el Sector público (Administraciones públicas y el resto de las entidades que lo integran) recobra un papel proactivo muy relevante. Y ello se explica, porque estamos ante sujetos (públicos) que también actuarían como gestores y emisores o suministradores, amén de demandantes o receptores de datos. En todo caso, hay que tener en cuenta que estos sujetos son reconocidos como fuentes de valiosa información o datos fiables; esto es, útiles o muy valorados por otros tipos de agentes u operadores que actúan en un mercado competitivo. Por tanto, es claro que en el caso del sector público se trataría de sujetos principales a los efectos examinados.

4.1. El deber de tutela pública reforzada en el caso de derechos fundamentales, protección de datos y privacidad

La gobernanza de datos o *data governance,* por las razones expuestas supra, *hoy es -o debería ser- pieza nuclear en toda organización y modelo de gestión. Como tal, implica de forma necesaria fijar una clara política* estratégica en materia de datos para asegurar la "buena administración" y diseñar una adecuada política orientada a la gestión responsable de datos.

En todo caso, será fundamental establecer herramientas destinadas a la protección eficaz de los datos, conforme a lo dictado en la vigente legislación europea y nacional complementaria, artículo 24 del Reglamento general de protección de datos (RGPD), en el cual, de forma expresa, se determina la *responsabilidad del responsable del tratamiento*; asimismo, de acuerdo con lo expresado sobre esta cuestión en el Considerando 78, donde se dice *La protección de los derechos y libertades de las personas físicas con respecto al tratamiento de datos personales exige la adopción de medidas técnicas y organizativas apropiadas con el fin de garantizar el cumplimiento de los requisitos del presente Reglamento. A fin de poder demostrar la conformidad con el presente Reglamento, el responsable del tratamiento debe adoptar políticas internas y aplicar medidas que cumplan en particular los principios de protección de datos desde el diseño y por defecto (...)*. Todo ello, en suma, en atención a lo declarado con carácter previo en el texto de la Carta de los

[42] Compartiendo lo expuesto, de forma magistral, por Beltrán Castellanos, J.M. (2024): *La brecha digital en las relaciones de la ciudadanía con las Administraciones públicas*. Tirant lo Blanch, Valencia.

[43] En efecto, es en este objetivo de "desbloquear datos" para asegurar su libre tráfico o circulación donde la Estrategia Europea de Datos hace hincapié; por lo que su logro, en la práctica, resultaría clave. Cuestión distinta es la problemática técnica o jurídica que conllevaría su implementación, amén de afrontar/tratar diversos riesgos regulatorios, tecnológicos, operativos, entre otros.

Derechos Fundamentales de la UE[44], donde se reconoce el derecho de los ciudadanos de la Unión a contar con la debida tutela, garantizando la protección de su privacidad y datos personales.

Por tanto, como ha sido argumentado, los datos se han convertido en una materia prima, activo o recurso clave para cualquier organización o empresa. Por ello, es principal asegurar, con una adecuada gestión de aquellos, así como prevenir, su tratamiento ante posibles riesgos. Y, en todo caso, a dichos efectos, se precisa disponer de los oportunos recursos, medios humanos y materiales, así como de la capacitación profesional o formación especializada –incluyendo, la técnica y específica jurídica-. Esto es, en la práctica, toda entidad u organización se debería asegurar de que dispone de la capacidad suficiente para el correcto tratamiento de los datos, y el específico que proceda en atención a cada tipo de dato. Pues, para poder "crear valor" a partir de los posibles "datos originales" o "datos-fuente" obtenidos en cada caso, antes es necesario saber procesarlos o tratarlos. Con base en lo señalado, también podría ser esencial aumentar la eficacia y la eficiencia en los procesos de toma de decisiones al respecto, así como en orden al adecuado diseño de los modelos de gestión de datos que deben ser implementados.

Como se sabe, la tecnología actual facilita que distintos operadores o empresas del sector privado, así como también las Administraciones Públicas y otras entidades del sector público, obtengan y puedan usar datos personales, asimismo, para su posterior aplicación o reutilización en orden a sus competencias, funciones y actividades. Lo mencionado es fruto de la transformación digital y del aumento de los servicios digitales, pero, también supone la generación de mayores riesgos. Por ello, se presentan nuevos retos en este terreno.

En consecuencia, en la actualidad, estimamos que es de sumo interés reforzar las medidas preventivas y destinadas a la protección, siendo esta cuestión prioritaria. Ello, parece conveniente a la luz de la evolución tecnológica, de la digitalización y de la libre circulación de datos que concurre. En definitiva, el desarrollo del mercado digital europeo obliga a tener en cuenta todo lo mencionado, si bien, desde la óptica jurídica, aún se plantean complejos desafíos[45].

Lo cierto es que la economía digital se posiciona de forma progresiva, por lo cual, es necesario contar con una robusta arquitectura legal en materia de datos. Y, en este sentido, cabe significar la funcionalidad fundamental del actual Sistema europeo de gobernanza de datos. Así, ante el escenario electrónico y "horizonte digitalizado" que se abre, toda organización (entidad pública o privada) ha de adoptar medidas adecuadas y en orden al cumplimiento de la legislación, también para prevenir o afrontar amenazas o riesgos con eficacia. Con lo cual, también resultará de interés la implementación efectiva de adecuados sistemas integrados de gestión de datos y gestión de riesgos, así como de instrumentos tecnológicos y medidas orientadas a la ciberseguridad[46]. De este modo, también por parte del actual legislador se ha de tratar de reforzar las medidas de protección preexistentes, a su vez, aportando confianza y seguridad jurídica.

Resulta conveniente avanzar, de ello no hay duda, adaptando los clásicos instrumentos técnicos y jurídicos de protección previstos por el Ordenamiento a los nuevos tiempos de la era digital. Ahora bien, no limitando las obligaciones o el deber de diligencia exigido o exigible a las entidades u operadores; y, en particular, por lo que corresponde a los sujetos responsables del tratamiento de datos. Así, se deberá estar preparado para responder de forma satisfactoria y con celeridad ante el incremento del riesgo, lo cual implica aportar una tutela reforzada o específica según cada supuesto. En este sentido, no se puede ignorar que el aumento de las prácticas digitales es ya un hecho y, con ello, se produce mayor circulación de datos en el entorno global y tecnológico.

Lo señalado sirve para razonar que se ha de prestar máxima protección a los datos personales, también se ha de brindar una tutela específica a otros tipos de datos no personales, según cada supuesto, categoría o valor. Y, a dicha finalidad, consideramos que se debería aumentar la legislación vigente en aras de garantizar una óptima tutela jurídica en materia de datos, y no solo por lo que respecta a los calificados como "datos personales". Ello, sobre todo, actuando de forma preventiva y con eficacia, ante las posibles amenazas que afectaran a la intimidad o privacidad de las personas[47]. Además, en este escenario de tráfico digital incrementado, hay que tener en cuenta que también hay otros datos (no personales) que pueden adquirir alto valor, y son dignos de especial protección. En virtud de lo apreciado, resulta razonable que la protección de las distintas tipologías de datos se convierta, en la actualidad, en una cuestión de máximo interés. Y, por ende, desde el Ordenamiento se debe dar una respuesta eficaz al respecto, así como ofrecer óptima tutela pública.

---

44 Cfr. Carta de los derechos fundamentales de la Unión Europea, https://www.boe.es/doue/2010/083/Z00389-00403.pdf.

45 Al respecto, vid., AEPD (2023): "Aproximación a los espacios de datos desde la perspectiva del RGPD", https://www.aepd.es/guias/aproximacion-espacios-datos-rgpd.pdf

46 La UE trabaja para promover la "ciberresiliencia" y proteger los datos con el fin de ofrecer seguridad a la sociedad y la economía en línea, vid., al respecto, el nuevo Reglamento de Ciberresiliencia, Reglamento (UE) 2024/2847 del ParU lamento Europeo y del Consejo (DOUE L 2024/2847, de 20.11.2024), https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=OJ:L_202402847, y documentación en https://eur-lex.europa.eu/ES/legal-content/summary/the-eu-cybersecurity-act.html

47 En nuestra opinión, es necesario disponer de una cobertura legal óptima en este terreno, con el fin de asegurar las necesarias garantías y seguridad jurídica. En todo caso, dotando de una específica protección (máxima) a los derechos fundamentales, privacidad y protección de los datos personales. También, por otra parte, es de interés ofrecer el necesario amparo jurídico a otro tipo de datos "no personales". Pues, con respecto a estos últimos, conviene recordar que son dignos de especial tutela jurídica aquellos otros datos o información sujeta o relacionados con determinados derechos o intereses legítimos, como pueden ser los amparados por Derecho de la propiedad intelectual/industrial, u otras informaciones o datos confidenciales o ligados a secretos empresariales, entre otros posibles.

4.2. La protección de otros derechos y tipologías de datos (datos no personales)

Más allá de la necesaria protección con que ya se dota a los datos de carácter personal por la vigente legislación europea, y siendo -además- un modelo muy reconocido a nivel internacional, también conviene tener en cuenta que otros tipos de datos pueden requerir una tutela específica, en la actualidad o a futuro, dado el amplio desarrollo digital y el tráfico de datos. Por ello, en materia de gestión de datos, consideramos que conviene contar con un sistema eficaz de protección integral. Y, en este sentido, implementar medidas que específicamente estén destinadas a dotar de mayor tutela a los derechos de propiedad intelectual e industrial; esto es, en atención a prevenir los nuevos riesgos de la era digital. Ello, en interés de ofrecer mayores garantías y, de forma específica, en aras de aportar la necesaria tutela a los derechos e intereses legítimos relativos a las distintas modalidades de activos intangibles, ya que estos también son dignos de especial atención y custodia, al ser su valor clave en términos económicos, competitivos y estratégicos.

Así pues, desde la UE, podría ser conveniente hacer mayor hincapié en esta cuestión, toda vez que el valor de los derechos de la propiedad intelectual/industrial es cada vez más reconocido, asimismo, como activo intangible y por sus implicaciones positivas, en atención a promover o fomentar varios aspectos ligados a la I+D+I, entre otros, la actividad económica, la inversión, la competitividad, la sostenibilidad, el empleo, etc. En su defecto, podrían incrementarse los riesgos de incidencias o impactos adversos, por ejemplo, ante posibles ilícitos, amenazas o acciones que supongan vulnerar la propiedad intelectual e industrial.

Al respecto, a modo de ejemplo sobre el interés de esta cuestión, cabe citar que ya fueron planteadas algunas iniciativas europeas en el pasado, como el Plan de acción en materia de propiedad intelectual e industrial de 2020[48], donde la Comisión pretendió mejorar las medidas de tutela de la propiedad intelectual e industrial. En este sentido, véase el Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo, para hacer frente a los posibles contenidos ilícitos en línea[49]. También, a través de varias herramientas que se establecen contra la falsificación, la Recomendación (UE) 2024/915 de la Comisión, de 19 de marzo de 2024, sobre medidas destinadas a luchar contra la falsificación y a reforzar la observancia de los derechos de propiedad intelectual e industrial[50].

No obstante, consideramos que en el presente conviene insistir más en este tipo de acciones. Además, sí sería muy importante avanzar en lograr mayor colaboración y cooperación más eficaz entre todas las partes: titulares de derechos, prestadores de servicios intermediarios y autoridades competentes, organismos de control o supervisión. Todo ello, con objeto de asegurar buenas prácticas en el mercado digital, óptimas y más responsables, así como por lo que respecta al empleo adecuado de medios tecnológicos o IA, entre otras acciones.

A su vez, la supervisión pública de todo ello resultará esencial, así como la previa evaluación y prevención del riesgo, también en orden a garantizar la posible imputación de sus posibles efectos adversos y la procedente atribución de responsabilidades por daños o perjuicios causados. Sumado a ello, la mejora en el intercambio de información actualizada por parte de las autoridades de control competentes es clave. Asimismo, desde la perspectiva del operador, es preciso actuar de forma proactiva (proactividad responsable), contar con un adecuado sistema de gestión del dato, disponer de equipos profesionales o contar con una formación especializada en este ámbito. Lo mencionado hoy son presupuestos esenciales -desde el punto de vista estratégico y operativo-, para toda entidad pública o privada, empresa u organización de todo tipo. Y ello, no solo por lo que respecta al tratamiento y empleo de datos personales, también de otras modalidades, con el fin de prevenir vulnerar información protegida o derechos de la propiedad intelectual e industrial, entre otras clases de datos o activos intangibles.

5. Conclusiones

Los datos son, en la actualidad, un activo intangible muy apreciado, recurso clave para el mercado digitalizado de datos y, a su vez, para el entrenamiento y funcionamiento de la inteligencia artificial (IA). Reconociendo dicho valor, la Comisión Europea ha trazado una ambiciosa planificación estratégica, la Estrategia Europea de Datos. Ello, con el principal objetivo de encaminar el desarrollo de políticas y medidas concretas que propicien el buen desarrollo del mercado europeo de datos en la Unión Europea (UE) y, por ende, del mercado digital. Pues hoy ambas realidades quedan vinculadas de forma inexorable.

A dicha finalidad, en los últimos años y de forma progresiva, el legislador europeo ha dictado una serie de instrumentos normativos en el ámbito del derecho digital y la gobernanza de los datos de distinta tipología. Amén del pionero Reglamento General de Protección de Datos (RGPD 2016), el cual, hasta la fecha, rige en materia específica de datos personales. Esta normativa, digno es reconocer, marcó un hito jurídico en el Ordenamiento común europeo. Además, es importante destacar que ya, en el propio RGPD, el legislador europeo ha reconocido el impacto que en esta materia representa la ágil evolución tecnológica

[48] La Comisión publicó el 25 de noviembre de 2020 un Plan de acción sobre propiedad intelectual e industrial con el objetivo de ayudar a las pequeñas y medianas empresas (pymes), en lo relativo a sus invenciones y creaciones, así como propiciar mejoras. También, de este modo, generar beneficios en interés colectivos, económicos y sociales. Para más información al respecto, vid., Comisión europea: (2020): "Cómo aprovechar al máximo el potencial innovador de la UE: un plan de acción en materia de propiedad intelectual para apoyar la recuperación y la resiliencia de la UE", fecha doc. 24/11/2020, https://ec.europa.eu/docsroom/documents/43845; https://stopfalsificaciones.oepm.es/novedades-y-publicaciones/novedades/La-Comision-Europea-adopta-un-Plan-de-accion-sobre-propiedad-intelectual-e-industrial-para-reforzar-la-resiliencia-y-la-recuperacion-economicas-de-la-UE/

[49] Reglamento (UE) 2022/2065 del Parlamento europeo y del Consejo de 19 de octubre de 2022 relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Reglamento de Servicios Digitales). L 277, de 27.10.2022.

[50] DOUE L núm. 915, de 26 de marzo de 2024.

y el fenómeno de la globalización. También, supone un incremento de riesgos.

Por lo cual, convendrá afrontar los nuevos retos con éxito, si bien, en todo caso, se ha de garantizar la debida protección de la información y, en particular, de los datos personales, de acuerdo con lo dictado por el Ordenamiento vigente. En este sentido, en particular, es oportuno recordar y tener presente, entre otros, el Considerando 6 del RGPD. Asimismo, haciendo referencia al desarrollo de la economía digital, se hace hincapié en el deber de *reforzar la seguridad jurídica y práctica para las personas físicas, los operadores económicos y las autoridades públicas* (Considerando 7 del RGPD).

De este modo, a fecha actual, cabe identificar como principales pilares normativos, básicos y aplicables de forma preceptiva, en concreto y por lo que respecta a la gestión y el tratamiento de los datos -personales y no personales-, tres Reglamentos (UE) o "Leyes UE", a saber, el RGPD (2016), el Reglamento de gobernanza de datos (*Data Governance Act*, 2022) y el Reglamento sobre normas armonizadas para un acceso justo a los datos y su utilización (*Data Act*, 2023). Asimismo, de forma adicional, cabe agregar el más reciente, Reglamento relativo al Espacio Europeo de Datos de la Salud (2025).

Dada la importancia de estas normativas específicas -entre otras de interés-, se ha realizado expresa referencia a las mismas en este trabajo, tanto por estar en relación directa con el objeto del presente estudio como por verse afectadas -y de forma muy significativa- por las nuevas propuestas regulatorias planteadas por la Comisión Europea, vía el actual paquete normativo Ómnibus Digital presentado en 2025.

Con todo, ahora, nos encontramos con este nuevo paquete normativo "Ómnibus Digital" que supone reformas muy relevantes en varias "Leyes UE", entre otras las precitadas. Esta reciente iniciativa regulatoria, sin duda, adquiere gran interés técnico y jurídico, motivo por el cual ha sido analizada y valorada en este texto. Si bien, quedamos a la espera del resultado final del procedimiento legislativo en curso, así como de los debates que tengan lugar durante el mismo, hasta conocer el texto legal definitivo que sea adoptado.

Resulta evidente que se aborda una cuestión regulatoria compleja, por las razones expuestas en este trabajo. Siendo, además, de gran importancia, no solo desde el punto de vista jurídico, también por su posible impacto social y económico. Por ende, cabe pensar que no será fácil alcanzar el consenso sobre este tema, al concurrir diversos intereses en conflicto, por lo que podrían presentarse enmiendas o efectuarse modificaciones respecto a lo inicialmente propuesto por la Comisión, y en aras de poder llegar a un acuerdo. Por tanto, se deberá atender al curso de las posibles discusiones que se desarrollen en las instituciones europeas, al ser examinadas las propuestas de reforma del "Ómnibus digital" planteadas por la Comisión, también por el Parlamento y el Consejo.

El tema, por tanto, no es baladí, al implicar cambios radicales en la normativa preexistente. Las reformas planteadas en el actual sistema jurídico aplicable en materia de datos responderían -según se infiere- a una finalidad principal, en resumen, promover, con celeridad, la economía del dato como paradigma, facilitar el cumplimiento legal y promover la implementación de la IA. A dichos efectos, se realizaría una trasformación radical en la disciplina común que había sido consolidada en el Derecho europeo. Pues, como ha sido analizado, afectaría a varias Leyes UE.

Así pues, cabe observar que hoy asistimos a lo que podría considerarse como un giro radical en el enfoque regulatorio que se había seguido hasta la fecha. Los cambios propuestos por la Comisión, a su vez, son realizados en consonancia con el nuevo rumbo que se traza desde la UE, cuyo faro guía es la economía impulsada por datos o *data driven economy*. Conforme a dicho horizonte, ahora, parece que se hace primar este paradigma económico. Por lo cual, el máximo interés quedaría centrado en lograr una mayor disponibilidad de distintos tipos de datos, dinámicos y accesibles. Asimismo, a este escenario se suma la útil funcionalidad instrumental de la IA -o de diversos sistemas basados en la IA-, por lo que surge el interés añadido de fomentar su desarrollo y facilitar su aplicación. Estos, en síntesis, parecen ser o se configurarían, en términos estratégicos, como los actuales "intereses preferentes o prioritarios" europeos,.

Todos estos factores conforman un entorno digital complejo desde la óptica jurídica, si bien dicha realidad pretende ser regulada con éxito. Desde luego, esta misión no será tarea fácil o, al menos, sin poner en riesgo algunas de las garantías y derechos que ya habían sido consagrados por el Estado de Derecho. Al respecto, cabe reseñar, lo relativo a derechos fundamentales, como son la protección de datos y la privacidad, además de otros posibles derechos e intereses legítimos que merecen una tutela específica.

Ergo, es claro que ante los nuevos desafíos se ha de contar con una regulación avanzada y adecuada, pero, sobre todo, también garante de la seguridad jurídica y de los derechos de los ciudadanos. Por ello, siendo coherentes, cabe reflexionar sobre la importancia de lograr el necesario y justo equilibrio entre intereses privativos y colectivos que son principales. Esto es, entre la esencial protección que ha de ser otorgada a los datos y el pretendido liderazgo del mercado digital. A dicho fin, resultaría deseable la posible conciliación de los objetivos estratégicos precitados, toda vez que promover el emprendimiento innovador y tecnológico puede ser perfectamente compatible con la tutela de los datos. Esta última, en nuestra opinión, ha de ser asegurada en todo caso.

Por ello, no parece conveniente reducir el nivel de exigencia con respecto a las obligaciones que vienen siendo requeridas en materia de tratamiento de datos, ni tampoco con respecto a las garantías jurídicas previstas por el Ordenamiento UE en lo relativo a la protección de los datos personales o de otra tipología, como son -por ejemplo- los relativos a derechos de la propiedad intelectual o industrial, toda vez que se trata de activos intangibles que merecen digna tutela pública. Así pues, el deber de cumplimiento legal exigido o exigible ha de ser óptimo. Y no es algo antagónico con el interés de impulsar el desarrollo de la innovación tecnológica, ni una competitividad responsable y eficiente. Además, en términos de viabilidad jurídica, parece más razonable promover

buenas prácticas, seguras y proactivas, sin incrementar los riesgos de distinta tipología (regulatorios, tecnológicos, operativos y estratégicos, entre otros). Sobre todo, teniendo en cuenta el contexto global y la propia dinámica que caracteriza al entono digital, la intensa circulación o las posibles transferencias de información o datos. Agregado a ello, no se puede ignorar que no resultará sencillo asegurar su control, al coexistir múltiples entornos o ecosistemas digitalizados, europeos e internacionales.

Por otra parte, resulta algo paradójico que en estos momentos y aprovechando este impulso de reforma regulatoria, amplia y difusa, vía el actual "Ómnibus Digital" presentado por la Comisión, no sean también abordadas otras cuestiones esenciales en materia de protección de datos. Aspectos que, todavía, convendría concretar o aclarar más, al no disponer -hasta la fecha- de una noción positivizada precisa o con suficiente cobertura legal. En este sentido, por ejemplo, resultaría de interés que fuera precisado todo lo relativo a la titularidad de los datos. Ello parece ser sustancial, por lo que merece especial atención, al objeto de que pudiera quedar establecido un régimen claro y común acerca de la titularidad del dato. Esto es, a modo de contar con un estatuto básico, propio y aplicable al genuino titular de los datos que son obtenidos, empleados o digitalizados. Lo señalado, sobre todo, podría ser muy útil, teniendo en cuenta la dinámica económica proyectada, el aumento en la circulación de datos que acontece en el mercado digital, la diversidad de usos o reutilización de los mismos y la concurrencia de diferentes sujetos u operadores intervinientes, *v.gr.,* posibles suministradores o proveedores de servicios, entre otros. Además, lo advertido no es baladí, ante las eventuales aplicaciones de sistemas basados en IA y que, como se conoce, para su entrenamiento requieren ser nutridos con gran cantidad de información o de datos de calidad. Por todo ello, estimamos que sí podría ser de gran interés jurídico lo mencionado, en aras de delimitar o concretar la figura del titular del dato *strictu sensu,* asimismo, por lo que respecta a sus derechos o facultades. En suma, parece esencial determinar un régimen específico de titularidad para este derecho de propiedad y tipología de bien o activo intangible. Así pues, convendría que pudiera ser fijado por el legislador europeo, de forma nítida, uniforme y eficaz. Esta es, por tanto, a nuestro juicio, una cuestión que aún queda pendiente o por abordar en el Derecho digital.

En definitiva, a modo de valoración final, estimamos que si bien, *a priori*, con el paquete normativo Ómnibus digital puede concurrir un buen propósito por parte de la Comisión Europea, no parece que sea razonable retroceder en lo ya alcanzado o regulado por el Ordenamiento jurídico común europeo. En especial, en orden a la debida tutela de los datos que se espera, y ha de regir, en todo caso. Máxime, en el contexto digital actual y frente a nuevos paradigmas económicos o tecnológicos que surgen.

Por ello, cabe propugnar que la seguridad jurídica ha de primar. La legislación ha de generar confianza, aportando certeza legal, solidez y garantías jurídicas suficientes. Así, consideramos que resulta esencial propiciar el equilibrio entre la protección de los derechos -por ende, de los datos- y el interés de promover la economía digital o el mercado digital. Ergo, se ha de buscar la justa equidad y la proporcionalidad en las normativas y medidas de actuación que fueran adoptadas o encaminadas, pues, solo así -se infiere- podrán ser anfrontados con éxito los nuevos retos.

Referencias bibliográficas

Agencia Española de Protección de Datos, AEPD (2021), "Gestión del riesgo y evaluación de impacto en tratamientos de datos personales", 29 de junio de 2021. Disponible en: https://www.aepd.es/guias/gestion-riesgo-y-evaluacion-impacto-en-tratamientos-datos-personales.pdf (Fecha consulta:10/02/2026).

Agencia Española de Protección de Datos, AEPD (2018): "Guía del Reglamento General de Protección de Datos para responsables de tratamiento". AEPD, Madrid. Disponible en: https://www.aepd.es/media/guias/guia-rgpd-para-responsables-de-tratamiento.pdf (Fecha última consulta: 20/02/2026).

Agencia Española de Protección de Datos, AEPD (2020): "Guía de Protección de Datos por defecto", 8 de octubre de 2020. https://www.aepd.es/guias/guia-proteccion-datos-por-defecto.pdf (Fecha consulta: 10/02/2026).

Agencia Española de Protección de Datos, AEPD (2023): "Aproximación a los espacios de datos desde la perspectiva del RGPD", https://www.aepd.es/guias/aproximacion-espacios-datos-rgpd.pdf (Fecha consulta: 11/02/2026).

Aguilar Alonso, I. y Lluesma Rodrigo, P. (2019). Una introducción al *sandbox* regulatorio, *Actualidad jurídica Uría Menéndez*, 52, pp. 95-100. https://www.uria.com/documentos/publicaciones/6676/documento/foro05.pdf?id=8961&forceDownload=true (fecha consulta: 10/02/2026).

Barnés Vázquez. J. (1998): El principio de proporcionalidad. *Cuadernos de Derecho Público* - Instituto Nacional de Administración Pública, 5. Recuperado a partir de https://revistasonline.inap.es/index.php/CDP/article/view/509 (Fecha consulta: 11/02/2026).

Barrio Andrés, M. (2024): Los principios estructurales del Reglamento General de Protección de Datos. *Actualidad jurídica iberoamericana*, 20, 2024, pp. 1322-1341. Disponible en: https://revista-aji.com/wp-content/uploads/2024/02/AJI20_Art_42.pdf.

Beltrán Castellanos, J.M. (2024): *La brecha digital en las relaciones de la ciudadanía con las Administraciones públicas*. Tirant lo Blanch, Valencia.

Cerrillo i Martínez, A., dir. (2022): *La administración digital.* Dykinson, Madrid.

Dopazo Fraguío, M.P. (2025): "´Tráfico digital de datos: Consideraciones sobre la actual cobertura legal europea. ¿Tutela pública suficiente?", en Candelario, M.I. (Dir.), *La propiedad industrial entre la digitalización, la innovación y la sostenibilidad.* Tirant lo Blanch, Valencia 2025 (Capítulo 6, págs. 143-197). https://doi.org/10.36151/TLB_9791370109493.

Dopazo Fraguío, P. (2019): Protección de datos y derechos digitales: arquitectura del nuevo binomio regulatorio. *Derecom: Revista Internacional de Derecho de la Comunicación y las Nuevas Tecnologías*, 26, pp. 17-48.

Dopazo Fraguío, P. (2022): El nuevo reglamento europeo para la gobernanza del dato: ¿Liberación segura de información y neutralidad de su tratamiento?". *REDE, Revista española de derecho europeo*, 82, 2022, pp. 115-166.

González Mendoza, D.P. (2025): Los datos biométricos y las tecnologías que los utilizan para su funcionamiento: Régimen jurídico aplicable y potenciales riesgos. *Revista Vasca de Administración Pública* (RVAP), 132, pp. 427-464.

González Mendoza, D.P. (2024): *El alcance del derecho a la protección de datos personales en las administraciones públicas*. Aranzadi, Cizur Menor.

Guasch Portas, V. y Soler Fuensanta, J.R. (2015): El interés legítimo en la protección de datos. RDUNED, *Revista de Derecho UNED*, 16, pp. 417-438. Disponible en: https://revistas.uned.es/index.php/RDUNED/article/view/15245 (Fecha consulta: 10/02/2026).

INCIBE: "NIS2: lo que necesitas saber", en: https://www.incibe.es/incibe-cert/sectores-estrategicos/NIS2-necesitas-saber (Fecha consulta: 14/03/2026).

INCIBE (2020): "Tecnologías disruptivas para la empresa segura. Instituto Nacional de Ciberseguridad", 2020, https://www.incibe.es/empresas/blog/tecnologias-disruptivas-empresa-segura. (Fecha consulta: 20/02/2026).

KPMG (2023): "RGPD y las claves de la responsabilidad proactiva para su aplicación", 18 mayo 2023, https://www.tendencias.kpmg.es/2023/05/rgpd-claves-responsabilidad-proactiva-aplicacion/ (Fecha consulta:11/02/2026).

López Calvo, J., coord. (2019): *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD*. Wolters Kluwer España, Madrid.

López-Lapuente, L. (2023): La nueva regulación europea de los datos: cómo dar forma al futuro digital de Europa". *Actualidad Jurídica Uría Menéndez*, 61, pp. 50-71. https://www.uria.com/documentos/publicaciones/8346/documento/AJUM_61.pdf?id=13294&forceDownload=true (Fecha consulta: 10/01/2026).

Menéndez González, N. (2024): Retos para la protección de datos en el uso de tecnologías de reconocimiento facial, en Pérez Díaz, R.; González Mendoza, D. P. y Vega García, P., *Perspectivas Transversales del Derecho a la Protección de Datos Personales*. Colex, A Coruña (pp. 131-143).

Moro Cordero, M.A. y Cerrillo i Martínez, A. (2024): El nuevo Reglamento sobre la Europa Interoperable en el marco de la estrategia europea de datos. *Consultor de los ayuntamientos y de los juzgados: Revista técnica especializada en administración local y justicia municipal*, 9.

Pérez de los Cobos Orihuel, F. (2018): *El derecho al respeto de la vida privada: los retos digitales, una perspectiva de Derecho comparado. Consejo de Europa*. EPRS, Servicio de Estudios del Parlamento Europeo, Bruselas, 2018. Disponible en: https://www.europarl.europa.eu/RegData/etudes/STUD/2018/628261/EPRS_STU(2018)628261_ES.pdf (Fecha consulta: 20/02/2026).

Piñar Mañas, J.L. (2025): *¿Quo vadis*, protección de datos?. *Revista de privacidad y derecho digital*, 36, pp. 19-24.

Piñar Mañas, J.L. (2020): Las claves de un derecho fundamental imprescindible. *El Cronista del Estado Social y Democrático de Derecho*, 88-89 (Ejemplar dedicado a: Protección de datos: antes, durante y después del coronavirus), pp. 6-19.

Razquin Lizarraga, M.M. (2024): Notas sobre el Dictamen 11/2024 del CEPD sobre uso del reconocimiento facial en el flujo de pasajeros en aeropuertos a la luz del Reglamento de Inteligencia Artificial y del RGPD", *Derecho Digital e Innovación*, 20.

Rodríguez Cembellín, D. (2025): Los *sandboxes* regulatorios y su uso en la regulación de la inteligencia artificial. *Revista General de Derecho Administrativo*, 70.

Romeo Casabona, C.M. (2021): Datos biométricos (Comentario al artículo 4.14 RGPD), en Troncoso Reigada, A. (Dir.), *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos Personales y Garantía de los derechos digitales.* Thomson Reuters Aranzadi, Cizur Menor (Vol. I, pp. 709-714).

Valero Torrijos, J. (2023): La reutilización de la información sanitaria desde la perspectiva de la regulación europea sobre gobernanza de datos. Andreu Martínez, B. (dir.), *Los datos de salud como eje de la transformación digital de la Sanidad.* Comares, Granada. pp. 45-68.