Revista de Derecho y Genoma Humano, 61 – enero-diciembre 2025

Law and the Human Genome Review

e-ISSN 2605-1230

https://doi.org/10.1387/rdgh.27342

Doctrina / Articles

El nuevo reglamento europeo relativo al espacio europeo de datos de salud: su impacto en la gobernanza del dato y su uso ético y seguro

Íñigo de Miguel Beriain*

Investigador. UPV/EHU

Ikerbasque, Basque Foundation for Science

Mercedes López de la Peña de Pablo

Magister en Derecho.

Mónica Loyo-Menoyo

Investigadora posdoctoral. UPV/EHU

Resumen: El objetivo de este texto consiste en analizar una norma recientemente publicada, pero de particular importancia, el Reglamento para un Espacio Europeo de Datos de Salud, en el ámbito del tratamiento de datos con fines de investigación e innovación. Nuestro enfoque parte de la idea de conectar este Reglamento con la Estrategia Europea de Datos y los principales instrumentos normativos elaborados a partir de ella, como la Directiva de datos abiertos y, especialmente, la Ley de Gobernanza de Datos, así como las herramientas encaminadas a asegurar la compartición de datos. El presente artículo incide de manera particular en la relación entre el Reglamento de Datos de Salud y la Ley de Gobernanza de Datos, incidiendo en las principales diferencias introducidas en el primero respecto al segundo.

Palabras clave: datos de salud, espacios de datos, interoperabilidad, usos secundarios, protección de datos.

Abstract: The aim of this text is to analyze a recently published but particularly important regulation, the Regulation for a European Health Data Space, in the field of data processing for research and innovation purposes. Our approach is based on the idea of connecting this Regulation with the European Data Strategy and the main regulatory instruments developed from it, such as the Open Data Directive and, especially, the Data Governance Act, as well as the tools aimed at ensuring data sharing. This article focuses in particular on the relationship between the Health Data Regulation and the Data Governance Act, highlighting the main differences introduced in the former with respect to the latter.

Key words: Health data, data spaces, interoperability, secondary uses, data protection.

Esta publicación se ha realizado en el marco del Grupo de Investigación del Sistema Universitario Vasco en Ciencias Sociales y Jurídicas aplicadas a las Nuevas Tecnologías (GI CISJANT, ref. IT1541-22), del proyecto «GODAS: Gobernanza de los usos secundarios de datos de salud y genéticos en espacios compartidos» (PID2022-137140OB-I00), financiado por el MCIN/AEI/10.13039/501100011033/FEDER, UE, concedido por la Agencia Estatal de Investigación española y del proyecto Carta de Derechos Digitales en el Ámbito de Entornos Específicos (ref C036/23-OT) financiado por Red.es y por la Unión Europea Next Generation EU.

*Email inigo.demiguelb@ehu.eus , ORCiD 0000-0002-2650-5280

1. Introducción

Decir que los datos constituyen, a día de hoy, uno de los principales insumos en la economía digital resulta tan reiterativo como cierto. Su existencia, unida al desarrollo de las nuevas capacidades de computación, ha hecho posible la revolución marcada por la inteligencia artificial, con todo lo que esto lleva consigo. Y todo ello, sin apenas costes, por cuanto, a diferencia de la mayoría de los recursos económicos, los datos pueden replicarse a un coste próximo a cero y su utilización por una persona u organización no impide la utilización simultánea por otra persona u organización. No obstante, todos estos logros sólo pueden alcanzarse si somos capaces de garantizar el acceso óptimo a los datos y su uso responsable.

Esta certeza ha estado presente en las iniciativas emprendidas por las instituciones europeas desde hace ya más de una década, pero fue sólo a partir de la publicación de la Estrategia Europea sobre Datos cuando se plasmaron en una línea de acción concreta. En este artículo mostraremos, en primer lugar, cuáles son las claves de esta visión, con especial enfoque en las normas que la han hecho posible, como la Ley de Gobernanza de Datos, por ejemplo. También explicaremos cuáles son las principales herramientas e instituciones creadas con el fin de desarrollar adecuadamente lo explicitado en estos instrumentos normativos. Finalmente, en la parte final del artículo nos referiremos a una norma que concreta en buena medida todo lo dispuesto sobre los espacios de datos a uno en concreto, el de datos de salud. Nos referimos, claro, al recientemente publicado Reglamento del Espacio Europeo de Datos de Salud.

2. El origen de la visión europea: la Estrategia Europea de Datos

La Comisión Europea empezó a adoptar medidas en torno a un tratamiento de datos capaz de conciliar el objetivo de maximizar los beneficios consustanciales a su utilización al menos desde 2014. Más tarde, con el Reglamento General de Protección de Datos (RGPD)[1], las instituciones europeas crearon un sólido marco normativo de defensa de los derechos e intereses de los ciudadanos europeos. A esta norma esencial habría que añadir después el Reglamento relativo a la libre circulación de datos no personales, el Reglamento sobre la Ciberseguridad[2], o la Directiva sobre datos abiertos[3]. Al mismo tiempo, las instituciones europeas trabajaron

[1] 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)
[2] REGLAMENTO (UE) 2019/881 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 17 de abril de 2019 relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) nº 526/2013 («Reglamento sobre la Ciberseguridad»)
[3] 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

duramente en el desarrollo de una legislación sectorial específica sobre el acceso a los datos en determinados ámbitos para hacer frente a las disfunciones de mercado identificadas. La Directiva sobre contenidos digitales[4], por su parte, había contribuido ya a la capacitación de las personas mediante la introducción de derechos contractuales cuando se prestaban servicios digitales a consumidores que facilitasen el acceso a sus datos.

No obstante, fue en febrero de 2020 cuando la Comisión Europea adoptó definitivamente una posición estratégica en este sentido. Fue entonces, de hecho, cuando hizo pública la Estrategia Europea de Datos, a través de una Comunicación al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones[5]. Dicha estrategia se basaba en el convencimiento firme de que el papel de liderazgo de la UE en la economía de los datos solo se fortalecería si se actuaba de manera inmediata, abordando de manera concertada cuestiones que iban desde la conectividad al tratamiento y almacenamiento de datos, la capacidad informática y la ciberseguridad. Además, la Comunicación señalaba que la UE tendría que mejorar sus estructuras de gobernanza para el manejo de datos y aumentar sus repositorios de datos de calidad disponibles para su utilización y reutilización. Esta idea era, a nuestro juicio, esencial de cara a entender cuáles eran las carencias de la UE en aquel momento y cuáles deberían ser los movimientos a emprender para afrontarlas[6].

La respuesta global a esta inquietud fue la aparición de un concepto, el espacio europeo de datos, que en la Estrategia se contemplaba como "un verdadero mercado único de datos, abierto a datos procedentes de todo el mundo, en el que los datos personales y no personales, incluidos los datos sensibles de empresas, estén seguros y las empresas también tengan fácil acceso a una cantidad casi infinita de datos industriales de alta calidad, de manera que se impulse el crecimiento y se cree valor, minimizando al mismo tiempo la huella humana medioambiental y de carbono. Debe ser un espacio en el que la legislación de la UE pueda aplicarse con eficacia y en el que todos los productos y servicios basados en los datos cumplan las normas pertinentes del mercado único de la UE"[7]. Con el fin de crear este espacio, la Estrategia subrayaba la necesidad de combinar una legislación y una gobernanza adaptadas al fin perseguido, de manera que se pudiera garantizar la disponibilidad de datos. Esto implicaría la creación de nuevas normas a añadir a las que ya hemos citado previamente, pero también la inversión en herramientas e infraestructuras, así como en competencias para el manejo de los datos. Todo esto debía guiarse por tres principios claros:

- Que los datos pudieran fluir en la UE y en todos los sectores,

[4] DIRECTIVA (UE) 2019/770 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 20 de mayo de 2019 relativa a determinados aspectos de los contratos de suministro de contenidos y servicios digitales
[5] Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Una Estrategia Europea de Datos. COM(2020) 66 final
[6] Véase a este respecto: Carvalho, G., Kazim, E. «Themes in data strategy: thematic analysis of 'A European Strategy for Data' (EC)». *AI Ethics* **2**, 53–63 (2022), https://doi.org/10.1007/s43681-021-00102-y
[7] Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Una Estrategia Europea de Datos. COM(2020) 66 final

- Que se respetasen plenamente las normas y los valores europeos, en particular la protección de los datos personales, la legislación en materia de protección de los consumidores y la legislación en materia de competencia.
- Que las normas de acceso a los datos y uso de estos fueran justas, prácticas y claras, que existan mecanismos claros y fiables de gobernanza de los datos, y que existiera un enfoque abierto, pero firme, en relación con los flujos internacionales de datos, basado en los valores europeos.

La manera en que la Estrategia quiso afrontar estos retos se basaba en cuatro pilares en los que se enfocaría su actuación: un marco de gobernanza intersectorial para el acceso a los datos y su utilización; inversiones en datos y refuerzo de las capacidades e infraestructuras de Europa para albergar, tratar y utilizar los datos, interoperabilidad; mejorar las competencias, empoderando a las personas e invirtiendo en cualificaciones y en pymes; y, por fin, promover el desarrollo de espacios comunes de datos europeos en sectores económicos estratégicos y en ámbitos de interés público. Esta última estrategia es precisamente la que constituye especial objeto de atención del presente texto, así que nos centraremos en ella.

De cara a lograr este objetivo estratégico, la Comisión propuso dividir el espacio único de datos en varios espacios concretos, atendiendo a las particularidades de los diferentes sectores implicados, de tal manera que pudiera haber un marco normativo horizontal, común a todos los espacios, que se complementaría, cuando procediese, mediante legislación sectorial relativa al acceso a los datos y su utilización, y a mecanismos para garantizar la interoperabilidad de los datos, de manera que los conceptos y modelos de gobernanza comunes pudieran reproducirse en los distintos sectores[8].

En ese primer momento, se identificaron nueve espacios: Espacio común europeo de datos relativos a la industria (fabricación); Espacio común europeo de datos relativos al Pacto Verde Europeo; Espacio común europeo de datos relativos a la movilidad; Espacio común europeo de datos relativos a la salud; Espacio común europeo de datos en materia financiera; Espacio común europeo de datos relativos a la energía; Espacio común europeo de datos relativos al sector agrario; Espacios comunes europeos de datos relativos a las administraciones públicas; Espacio común europeo de datos en materia de cualificaciones[9].

Finalmente, la Estrategia se marcaba el objetivo de impulsar decisivamente los trabajos sobre la Nube Europea de la Ciencia Abierta, una herramienta que estaría conectada y plenamente

[8] A mayor abundamiento, la Estrategia especificaba que "Las diferencias entre los sectores dependerán del nivel de desarrollo alcanzado en los debates acerca de la disponibilidad de datos en el sector y de los problemas detectados en relación con dicha disponibilidad. Otro factor pertinente es el grado de interés y participación del público en un sector determinado, que puede ser mayor en ámbitos como la salud o inferior en ámbitos como la fabricación. También debe tenerse en cuenta el posible uso intersectorial de los datos entre los diferentes sectores. Los espacios de datos se desarrollarán respetando plenamente las normas de protección de datos y con arreglo a las normas de ciberseguridad más elevadas disponibles." (Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Una Estrategia Europea de Datos. COM(2020) 66 final, Punto 5.D)

[9] A día de hoy, estos nueve espacios se han ampliado, hasta alcanzar la cifra de catorce, que puede incrementarse en un futuro. Véase Commission Staff Working Document on Common European Data Spaces, Brussels, 24.1.2024 SWD(2024) 21 final. Disponible *online* en: https://digital-strategy.ec.europa.eu/en/policies/data-spaces

articulada con los espacios de datos sectoriales y que debía ser capaz de garantizar la autonomía de la UE en la prestación de servicios europeos en la nube.

3. Normativa ligada al desarrollo de los espacios:

La Estrategia, con todo, no fue un mero brindis al sol, sino que trajo consigo una serie de iniciativas de particular importancia destinadas a implementarla. De cara a desarrollar adecuadamente los espacios de datos, las instituciones europeas han aprobado ya algunas normas absolutamente fundamentales. De entre ellas destacan por su particular relevancia tres: la Ley de Gobernanza de Datos[10], el Reglamento de Datos[11] y la Directiva de datos abiertos, ya citada anteriormente.

3.1.La Ley de Gobernanza de Datos

La primera de las normas que analizaremos aquí es la Ley de Gobernanza de Datos (LGD), que entró en vigor el 23 de junio de 2022 y es aplicable desde el 24 de septiembre de 2023 en la UE. Esta norma de esencial importancia de cara al desarrollo de los espacios de datos tiene por objeto facilitar el intercambio de datos en toda la UE y entre los diferentes sectores productivos, de manera que sea posible tanto generar crecimiento económico como aumentar el control y la confianza tanto de los ciudadanos como de las empresas en relación con sus datos. La LGD facilita el desarrollo de espacios comunes de datos europeos a través de la creación de varios agentes de particular importancia, que desarrollarán tareas fundamentales en el intercambio y el acceso a los datos.

En primer lugar, la LGD regula en su capítulo IV el altruismo de datos, estableciendo que los Estados miembros deberán poder aprobar disposiciones organizativas, técnicas o ambas que faciliten la cesión altruista de datos[12], como la disponibilidad de herramientas de fácil uso para que los interesados o los titulares de datos den su consentimiento o permiso para la utilización altruista de sus datos, la organización de campañas de sensibilización o un intercambio estructurado entre autoridades competentes sobre la forma en que las políticas públicas (por ejemplo, la mejora del tráfico, la salud pública y la lucha contra el cambio climático) se beneficien

[10] 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)

[11] 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)

[12] Esto es, "todo intercambio voluntario de datos basado en el consentimiento de los interesados para que se traten sus datos personales, o en el permiso de los titulares de datos para que se usen sus datos no personales, sin ánimo de obtener o recibir una gratificación que exceda de una compensación relativa a los costes en que incurran a la hora de facilitar sus datos, con objetivos de interés general tal como se disponga en el Derecho nacional, en su caso, como, por ejemplo, la asistencia sanitaria, la lucha contra el cambio climático, la mejora de la movilidad, la facilitación del desarrollo, elaboración y difusión de estadísticas oficiales, la mejora de la prestación de servicios públicos, la elaboración de políticas públicas o la investigación científica de interés general" (artículo 2.16)

de la cesión altruista de datos. A tales efectos, los Estados miembros deberán poder establecer políticas nacionales en materia de cesión altruista de datos (Considerando 45). Esta cesión se basará, generalmente, en el consentimiento de los interesados.

Al mismo tiempo, la norma da cuerpo de naturaleza a las organizaciones que realizan actividades de servicios basados en la cesión altruista de datos en la Unión, que no se consideran en ningún caso intermediarios de datos, en cuanto que sus servicios no están destinados a establecer relaciones comerciales entre los posibles usuarios de datos, por una parte, y los interesados y los titulares de datos que ceden los datos con fines altruistas, por otra. Estas entidades son esenciales para fomentar la aparición de conjuntos de datos de tamaño suficiente puestos a disposición sobre la base del altruismo de datos con el fin de permitir el análisis de datos y el aprendizaje automático, en toda la Unión[13]. La creación de un registro como el que se regula en los artículos 17 y siguientes del Reglamento es también esencial en este sentido.

En segundo lugar, a través de la regulación de la intermediación de datos[14] y del establecimiento de un estatuto jurídico para una nueva figura, los proveedores de servicios de intermediación de datos (DISP), en su Capítulo III. Estos son un tipo específico de intermediario de datos[15], definidos como un servicio cuyo objetivo es establecer «relaciones comerciales» para compartir datos. Por tanto, los servicios de intermediación están llamados a funcionar como organizadores fiables del intercambio o puesta en común de datos dentro de los espacios comunes europeos de datos[16]. Con tal fin, permitirán la puesta en común o el uso conjunto de datos entre unos agentes intervinientes y otros, así como el establecimiento de infraestructuras específicas para conectar a los interesados y a los titulares de datos con los usuarios de datos. Como orquestadores de los ecosistemas de puesta en común de datos, los intermediarios de datos abren el mercado en el contexto de los espacios comunes europeos de datos, otorgando seguridad a todo el sistema. Como dicen Michelli et al, “este nuevo marco se ha desarrollado para tranquilizar a los interesados/titulares sobre cómo se tratarán sus datos, es decir, sabrán que interactúan con un intermediario que gestiona sus datos de acuerdo con normas de

[13] Como dice el Considerando 50, las organizaciones en cuestión “han de poder recopilar los datos pertinentes directamente de las personas físicas y jurídicas o tratar los datos recopilados por terceros. El tratamiento de los datos recogidos podría ser realizado directamente por organizaciones de gestión de datos con fines altruistas para fines que ellas establezcan o, según proceda, podrían permitir el tratamiento por parte de terceros para esos fines. Cuando las organizaciones reconocidas de gestión de datos con fines altruistas sean las responsables o encargadas del tratamiento de datos tal como se definen en el Reglamento (UE) 2016/679, deben cumplir dicho Reglamento”.

[14] Como tal ha de entenderse, en general, “todo servicio cuyo objeto sea establecer relaciones comerciales para el intercambio de datos entre un número indeterminado de interesados y titulares de datos, por una parte, y usuarios de datos, por otra, a través de medios técnicos, jurídicos o de otro tipo, incluidos los servicios destinados al ejercicio de los derechos de los interesados en relación con los datos personales” (Artículo 2.11). La norma contiene excepciones que ahora no reflejaremos por limitaciones de espacio.

[15] Hay hasta seis tipos de intermediarios de datos. Véase al respecto: Micheli, M / Farrell, E / Carballa-Smichowski, B / Posada-Sanchez, M. /Signorelli, S / Vespe, *M*, *Mapping the landscape of data intermediaries— Emerging models for more inclusive data governance,* Publications Office of the European Union, Luxembourg, 2023, doi: 10.2760/261724, JRC133988

[16] Véase Data Governance Act explained, disponible *online* en https://digital-strategy.ec.europa.eu/en/policies/data-governance-act-explained [Última consulta: 15 de marzo de 2025]

seguridad estrictas, que no tiene ningún conflicto de intereses y que cumple plenamente la normativa aplicable de la UE"[17].

En tercer lugar, la LGD permitirá superar una situación que está provocando ciertas disfunciones a la hora de tratar los datos que han sido generados o recogidos por organismos del sector público u otras entidades con cargo a los presupuestos públicos. Y es que, si bien es cierto que la Directiva (UE) 2019/1024 y la normativa sectorial de la Unión garantizan que, en general, los datos generados por los organismos del sector público estén fácilmente disponibles para su utilización y reutilización; también lo es que determinadas categorías de datos (como los datos comerciales confidenciales, las informaciones amparadas por el secreto estadístico y los datos protegidos por derechos de propiedad intelectual de terceros, incluidos los secretos comerciales y los datos personales) a menudo no están disponibles en la práctica, ni siquiera para actividades de investigación o innovación de interés público. Y eso a pesar de que, como estamos señalando, podrían estarlo con arreglo al Derecho de la Unión aplicable, en concreto, con arreglo al Reglamento (UE) 2016/679 y las Directivas 2002/58/CE y (UE) 2016/680 (Considerando 6 de la LGD).

Antes de la aprobación de la LGD, la puesta a disposición de estos datos se demoraba sustancialmente, por los procedimientos implementados para garantizar el respeto de los derechos de terceros en torno a ellos o de limitar los efectos negativos sobre los derechos fundamentales, el principio de no discriminación y la protección de datos. Y dado que la normativa de referencia era una Directiva, había diferencias sustanciales entre los Estados miembros. Mientras algunos Estados estaban creando estructuras, estableciendo procedimientos o legislando para facilitar la reutilización de los datos, en otros no era así.

La LGD permite superar estas dificultades, señalando claramente que "el presente Reglamento debe aplicarse a los datos personales que no estén sujetos a la Directiva (UE) 2019/1024 en la medida en que el régimen de acceso excluya o restrinja el acceso a ellos por razones de protección de datos, privacidad e integridad de la persona, en particular de conformidad con las normas de protección de datos" (Considerando 10)[18]. Además, facilita sustancialmente la utilización de los datos para la investigación y la innovación europeas por entidades privadas y públicas, a través del establecimiento de unas condiciones claras para el acceso a tales datos y su utilización en toda la Unión, siguiendo los criterios expuestos en su Considerando 15.

[17] Micheli, M / Farrell, E / Carballa-Smichowski, B / Posada-Sanchez, M. /Signorelli, S / Vespe, M, Mapping the landscape of data intermediaries— *Emerging models for more inclusive data governance,* Publications Office of the European Union, Luxembourg, 2023, doi:10.2760/261724. Disponble en https://publications.jrc.ec.europa.eu/repository/handle/JRC133988

[18] Lo que, no obstante, no significa que a partir de su entrada en vigor exista una obligación de permitir la reutilización de los datos que obren en poder de organismos del sector público. El Considerando 11 de la DGA señala que "cada Estado miembro debe poder decidir, por lo tanto, si se proporciona acceso a los datos para su reutilización, así como sobre los fines y el alcance de dicho acceso. El presente Reglamento debe completar las obligaciones más específicas de los organismos del sector público de permitir la reutilización de datos establecidas en la normativa sectorial de la Unión o nacional, y debe entenderse sin perjuicio de estas obligaciones. El acceso del público a documentos oficiales puede considerarse de interés público".

Además, la LGD crea el registro europeo de datos protegidos en poder del sector público, disponible en data.europa.eu, el portal oficial de datos europeos[19].

Por fin, la LGD introduce algunos criterios fundamentales en torno al tratamiento de datos, estableciendo el criterio de que deberían cederse preferentemente los datos no personales, mientras que los datos seudonimizados, en general, podrían tratarse en entornos de tratamiento seguro, supervisados por el organismo del sector público que poseyera los datos, de forma que los derechos y los intereses de terceros queden protegidos. El criterio puede hallarse en el Considerando 15[20].

Es importante señalar, finalmente, que la LGD surge con vocación de ser una normativa marco, que puede ser perfectamente complementada por otras que se sitúen en sectores específicos. Su Considerando 3 señala que "la normativa sectorial de la Unión puede crear, adaptar y proponer elementos nuevos y complementarios, dependiendo de las particularidades de cada sector, como sucede con la normativa de la Unión prevista en torno a un espacio europeo de datos sobre la salud o el acceso a los datos integrados en los vehículos". Y, en todo caso, se ha de tener siempre presente que su ámbito no incluye la reutilización de datos protegidos relativos a las actividades que los Estados miembros efectúen en materia de seguridad pública, defensa y seguridad nacional, incluidos los datos obtenidos en procedimientos de contratación pública que entren dentro del ámbito de aplicación de la Directiva 2009/81/CE del Parlamento Europeo y del Consejo[21].

3.2. La Ley de Datos

El Reglamento de Datos[22] entró en vigor el 11 de enero de 2024. Será aplicable a partir del 12 de septiembre de 2025. Como segunda iniciativa legislativa clave anunciada en la estrategia europea de datos, el Reglamento de Datos complementa la Ley de Gobernanza de Datos. Su objeto de regulación, de hecho, es diferente pero complementario. La LGD regula los procesos y

[19] Es importante hacer notar que tampoco entran en el ámbito de aplicación de la DGA los datos de las empresas públicas. Como dice su Considerando 12, "La misión de servicio público puede definirse con carácter general o caso por caso para cada organismo del sector público. Puesto que las empresas públicas no se incluyen en la definición de organismo del sector público, el presente Reglamento no debe ser aplicable a los datos que obren en poder de empresas públicas. El presente Reglamento no debe ser aplicable a los datos que obren en poder de centros culturales, como bibliotecas, archivos, museos, orquestas, óperas, ballets y teatros, o por centros de enseñanza, ya que las obras y otros documentos que obren en su poder están protegidos principalmente por derechos de propiedad intelectual de terceros."

[20] Los datos personales solo han de transmitirse a un tercero para su reutilización cuando exista una base jurídica en la normativa en materia de protección de datos que lo permita. Los datos no personales solo deben transmitirse cuando no haya motivos para creer que la combinación de conjuntos de datos no personales conduzca a la identificación de los interesados. Esto debe aplicarse también a los datos seudonimizados que conserven su condición de datos personales. En caso de reidentificación de los interesados, debe exigirse una obligación de notificar dicha violación de la seguridad de los datos al organismo del sector público, además de una obligación de notificarla a una autoridad de control y al interesado de conformidad con lo dispuesto en el Reglamento (UE) 2016/679.

[21] En este sentido, el artículo 1.5. Especifica que "El presente Reglamento se entenderá sin perjuicio de las competencias de los Estados miembros respecto a las actividades relativas a la seguridad pública, la defensa y la seguridad nacional."

[22] 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)

estructuras que facilitan el intercambio voluntario de datos, mientras que el Reglamento de Datos aclara quién puede crear valor a partir de los datos y en qué condiciones. Como tal, este Reglamento está centrado especialmente en los datos generados a través del Internet de las Cosas[23], datos que en su mayor parte permanecen en poder de las empresas privadas[24], a fin de favorecer el intercambio de esos datos.

El instrumento clave del Reglamento de Datos para resolver este problema es la introducción de nuevos derechos de los usuarios de dispositivos IoT, de tal manera que puedan acceder a estos datos y compartirlos con otras empresas, gracias a una interoperabilidad claramente mejorada[25]. Esto debería dar más poder a los usuarios, permitirles beneficiarse más de los servicios adicionales y desbloquear los datos de la IoT para las empresas innovadoras[26]. También, además, se faculta su utilización por parte del sector público en los casos en los que sobrevenga una necesidad excepcional, por ejemplo en situaciones de emergencia pública, estableciendo normas claras sobre cómo deben presentarse dichas solicitudes[27].

En conexión con esto se halla una de las cuestiones fundamentales que el Reglamento pretende resolver: la del acceso a los datos generados por los dispositivos de IoT. A día de hoy es habitual que quienes desarrollan los sistemas de recogida y tratamiento de datos lo hagan de una forma que les favorezca claramente, primando sus intereses sobre los de los sujetos que generan los datos[28]. El Reglamento de Datos pretende acabar con esta situación de desequilibrio, garantizando "que los usuarios de un producto conectado o servicio relacionado en la Unión puedan acceder oportunamente a los datos generados por el uso de dicho producto conectado o servicio relacionado y que puedan utilizarlos, entre otros, compartiéndolos con terceros de su elección" (Considerando 5)[29]. Con tal fin, el Reglamento de Datos impone a los titulares de datos la obligación de ponerlos a disposición de los usuarios y de terceros elegidos por los usuarios en determinadas circunstancias, introduciendo así derechos que protegen a los usuarios frente a los

[23] Como dice el considerando 14, "Los productos conectados que, a través de sus componentes o sistemas operativos, obtengan, generen o recopilen datos relativos a su rendimiento, uso o entorno y que puedan comunicar dichos datos mediante un servicio de comunicaciones electrónicas, una conexión física o un acceso en el dispositivo, a menudo denominado «internet de las cosas», deben incluirse en el ámbito de aplicación del presente Reglamento, a excepción de los prototipos." Véase también a este respecto: Eckardt, M., & Kerber, W. (2024). «Property rights theory, bundles of rights on IoT data, and the EU Data Act». *European Journal of Law and Economics*, 57(1), pp. 113-143.

[24] El Considerando 63 especifica que "Aunque el concepto de «titular de datos» generalmente no incluye a los organismos del sector público, puede incluir a las empresas públicas. Las organizaciones que realizan actividades de investigación y las organizaciones que financian la investigación también se pueden organizar como organismos del sector público u organismos de Derecho público."

[25] Acerca de los posibles problemas y carencias de este enfoque, puede consultarse, por ejemplo: Drexl, J., et al. (2022). Position statement of the Max Planck institute for innovation and competition of 25 May 2022 on the Commission's Proposal of 23 February 2022 for a regulation on harmonized rules on fair access to and use of data (Data Act) (May 25, 2022). Max Planck institute for innovation & competition research paper No. 22–05. Retrieved February 26, 2022 from https://ssrn.com/abstract=413648, https://doi.org/10.2139/ ssrn.4136484 ; Kerber, W. (2023b). «Data Act and competition: An ambivalent relationship», *Concurrences* No.1–2023, pp. 30–36.

[26] Kerber, W, «Governance of IoT data: why the EU Data Act will not fulfill its objective». *GRUR International,* 72(2), pp. 120-135.

[27] Véase al respecto los Considerandos 63-65, así como el 70 y ss.

[28]Kerber proporciona buenos ejemplos en relación con esto en el sector de la automoción. Véase: Kerber, «Data-sharing in IoT ecosystems and competition law: The example of connected cars». *Journal of Competition Law & Economics, 15*, pp. 381–426.

[29] Véase a este respecto: Eckardt, M., & Kerber, W, «Property rights theory, bundles of rights on IoT data, and the EU Data Act». *European Journal of Law and Economics*, *57*(1), pp. 113-143.

excesos de poder de los desarrolladores[30]. También garantiza que los titulares de datos pongan los datos a disposición de los destinatarios de datos en la Unión en condiciones justas, razonables y no discriminatorias y de manera transparente.

En estrecha relación con la garantía de acceso está la necesidad de impulsar la interoperabilidad de los datos, habitual caballo de batalla en el campo de su uso. En este aspecto, el Reglamento también introduce medidas de particular importancia al establecer determinados requisitos esenciales de interoperabilidad en su tratamiento. Como dice el Considerando 103, a partir de la entrada en vigor del Reglamento, "los participantes en espacios de datos que ofrezcan datos o servicios basados en datos a otros participantes, que son entidades que facilitan o participan en el intercambio de datos dentro de espacios comunes europeos de datos, incluidos los titulares de datos, deben cumplir esos requisitos en lo que respecta a los elementos que estén bajo su control". No obstante, es probable que esto necesite un desarrollo normativo en sectores específicos[31].

Del mismo modo que la LGD, el Reglamento de Datos es una norma intersectorial, que no modifica las normas relativas al acceso a los datos existentes. No obstante, cualquier legislación futura debe ajustarse a sus principios. También de forma similar a la LGD, el Reglamento de Datos "no se aplica a los ámbitos que queden fuera del ámbito de aplicación del Derecho de la Unión y, en cualquier caso, no afecta a las competencias de los Estados miembros relativas a la seguridad pública, la defensa o la seguridad nacional, independientemente del tipo de entidad a la que los Estados miembros hayan confiado el desempeño de tareas en relación con dichas competencias, o de su facultad para salvaguardar otras funciones esenciales del Estado, incluida la garantía de la integridad territorial del Estado y el mantenimiento del orden público"[32].Tampoco afecta a las competencias de los Estados miembros en materia de aduanas y administración fiscal, ni a la salud y seguridad ciudadanas.

3.3. La Directiva sobre datos abiertos

La *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* (en adelante, DDA), modificó la vieja Directiva sobre estas materias, de 2003[33], actualizando el marco legislativo europeo vigente a partir los avances realizados en el mundo de la tecnología digital y

[30] Leistner, M./ Antoine, L. (2022). «IPR and the use of open data and data sharing initiatives by public and private actors, study commissioned by the European Parliament's Policy Department for citizens' rights and constitutional affairs at the request of the Committee on Legal Affairs». Disponible en: https://doi.org/10. 2139/ssrn.4125503

[31] Como la agricultura, por ejemplo. Véase: Atik, C,«Towards comprehensive agricultural data governance: Moving beyond the "data ownership" debate». *IIC-International Review of Intellectual Property and Competition Law, 53*, p. 701 y ss.

[32] Artículo 1.6. Esto, en realidad, cae de suyo teniendo presente la distribución competencial en el ámbito de la UE, que deja en manos de los Estados miembros todo lo relativo a materias como la seguridad pública, la defensa o la seguridad nacional.

[33] Directiva 2003/98/ CE del Parlamento Europeo y del Consejo de 17 de noviembre de 2003, relativa a la reutilización de la información del sector público.

participando en la estimulación de la innovación digital, especialmente la inteligencia artificial[34]. La DDA se basa en el principio general de que la información del sector público en poder de organismos públicos o empresas públicas, así como los datos de investigación financiados con fondos públicos, deben poder reutilizarse gratuitamente con fines comerciales y no comerciales. Además, los organismos del sector público están obligados a poner a disposición los datos dinámicos para su reutilización inmediatamente después de su recogida, a través de interfaces de programación de aplicaciones (API) adecuadas y, en su caso, como descarga masiva[35]. La única salvedad a este principio general es que el acceso a los datos se encuentre restringido o excluido por una norma nacional que regule el derecho de acceso a estos documentos o esté sometido a alguna excepción que marque la propia Directiva.

De esta forma, se invita a los Estados pertenecientes a la UE a que insten a sus organismos públicos a poner a disposición de sus ciudadanos los documentos de los que disponen para que puedan ser reutilizados por los interesados, así como promover e incentivar dicho mecanismo [36]. Con tal fin, se introducen conceptos como el de «datos dinámicos», esto es, «documentos en formato digital, sujetos a actualizaciones frecuentes o en tiempo real, en particular debido a su volatilidad o rápida obsolescencia» (artículo 2.8), o el de «conjuntos de datos de gran valor», descritos como aquellos cuya reutilización se asocia a importantes beneficios para la sociedad y la economía. Estos conjuntos de datos están sujetos a un conjunto independiente de normas que garantizan su disponibilidad gratuita, en formatos legibles por máquina, a través de API y, en su caso, como descarga masiva. La Directiva estimula en gran medida la puesta en común de estos conjuntos de datos[37]. La Directiva (UE) 2019/1024 incluía un plazo máximo de transposición fijado en el 17 de julio de 2021[38]. No obstante, no todos los Estados miembros la han traspuesto con la debida diligencia, lo que ha dado lugar a las disfunciones que la normativa ya analizada ha intentado paliar. Y a esto hay que añadir que la propia Directiva especifica que su articulado no se aplicará a las bibliotecas, incluidas las universitarias, los museos y los archivos, lo que excluye una parte importante de los datos disponibles. Tampoco se aplica a conjuntos de datos específicos de alto valor que obren en poder de empresas públicas, cuando ello provoque una distorsión de la competencia en los mercados correspondientes.

Hay, por fin, que señalar que la Directiva exigía que en un futuro se pudiera contar con una lista a escala de la UE de conjuntos de datos con un potencial particular para generar beneficios socioeconómicos, junto con condiciones de reutilización armonizadas. Esta exigencia acabó

[34] Véase el considerando 3 de la 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.

[35] Support Centre for Data Sharing (SCDS), *Analytical report on EU law applicable to sharing of non-personal data Support Centre for data sharing,* 2020, pp. 43-62. Disponible en: https://data.europa.eu/sites/default/files/course/EU%20law%20applicable%20to%20sharing%20of%20non-personal%20data.pdf

[36] Véase el considerando 23 de la Directiva (UE) 2019/1024.

[37] Support Centre for Data Sharing (SCDS), *Analytical report on EU law applicable to sharing of non-personal data Support Centre for data sharing*, 2020, pp. 43-62. Disponible *online* en: https://data.europa.eu/sites/default/files/course/EU%20law%20applicable%20to%20sharing%20of%20non-personal%20data.pdf.

[38] Así lo dispone el artículo 17.

tomando cuerpo a través del Reglamento de Ejecución (UE) 2023/138 de la Comisión de 21 de diciembre de 2022, por el que se establece una lista de conjuntos de datos específicos de alto valor y modalidades de publicación y reutilización. Dicho Reglamento especifica (artículo 3) que los organismos del sector público en cuyo poder obren los conjuntos de datos de alto valor que enumera en su anexo velarán por que los conjuntos de datos descritos o mencionados en el anexo estén disponibles en formatos legibles por máquina a través de las interfaces de programación de aplicaciones (API) que correspondan a las necesidades razonables de los reutilizadores. En el mismo artículo se especifica que esos organismos serán los encargados de establecer y publicar "las condiciones de uso de las API y los criterios de calidad del servicio sobre su rendimiento, capacidad y disponibilidad. Las condiciones de uso estarán disponibles en un formato legible por personas y por máquina. Tanto las condiciones de uso como los criterios de calidad del servicio serán compatibles con los acuerdos organizativos para la reutilización de conjuntos de datos de alto valor establecidos de conformidad con el artículo 4" del mismo Reglamento.

4. Herramientas de coordinación: el Data Spaces Support Centre y el Simpl (Smart Open-Source Middleware). Otras iniciativas

Con el fin de coordinar adecuadamente el desarrollo de los diferentes espacios de datos, las instituciones europeas están financiando, a través de sus programas de investigación, coordinación y apoyo, el desarrollo de una serie de organismos, estructuras y capacidades generales dedicadas a este fin. Entre ellas destacan tres: el Data Spaces Support Centre, Simpl: Smart Open-Source Middleware y el European Data Innovation Board (EDIB)

4.1. El Data Spaces Support Centre

Uno de los elementos esenciales para evitar que los diferentes espacios crezcan adecuadamente es, sin duda, la creación de una herramienta que coordine todas las acciones pertinentes sobre los espacios de datos sectoriales para garantizar que se desarrollen de forma coherente, sean interoperables y se beneficien de economías de escala mediante el uso de prácticas, componentes (denominados «componentes básicos») y herramientas comunes (por ejemplo, implementaciones de software o servicios que apliquen los componentes básicos mencionados que se consideren adecuados para su finalidad) [39]. Esta era, precisamente, una de las propuestas esenciales del primer programa de trabajo DIGITAL 2021-2228, que acabó dando lugar, en octubre, a una Acción de Coordinación y Apoyo (CSA) que ha creado y gestiona un

[39] Commission Staff Working Document on Common European Data Spaces, Brussels, 24.1.2024 SWD(2024) 21 final, p. 11.

Centro de Apoyo a los Espacios de Datos (DSSC) que, en principio, estará en funcionamiento hasta finales de marzo de 2026[40].

El DSSC tiene como objetivo determinar los requisitos comunes y establecer las mejores prácticas para acelerar la formación de espacios de datos soberanos como elemento crucial de la transformación digital en todos los ámbitos, proporcionando el mejor apoyo posible a las iniciativas de espacios de datos sobre los requisitos relacionados con los espacios de datos interoperables. Con ese fin, han formado una red de partes interesadas (stakeholders), con participantes procedentes de tres grandes grupos. En primer lugar, por las iniciativas europeas comunes sobre el espacio de datos financiadas por la UE (la Community of Practice (CoP)). En segundo lugar, un grupo de reflexión que apoya los objetivos de la CSD y ofrece recomendaciones sobre gobernanza y sostenibilidad (el Strategic Stakeholder Forum (SSF)). Por último, otras iniciativas y partes interesadas pertinentes para el desarrollo de espacios de datos.

Para apoyar el despliegue de espacios de datos, el DSSC ha desarrollado un kit de iniciación y un anteproyecto o blueprint. El blueprint consiste en un conjunto completo de directrices para apoyar el desarrollo de espacios de datos, que ahora mismo contiene un glosario, un modelo conceptual de espacio de datos y bloques de construcción, así como una recopilación de normas y estándares[41].

4.2. Simpl: Smart Open-Source Middleware

La labor realizada por el DSSC se complementará efectivamente gracias a la tarea emprendida por otra herramienta, Simpl, que es una plataforma de middleware de código abierto, que se empezó a desarrollar en enero de 2024, con el objetivo de garantizar que los espacios de datos se desplieguen sobre la base de una infraestructura técnica común[42]. Con tal fin se crearán tres diferentes productos, que serán los que utilicen todos los espacios de datos financiados en el marco de DIGITAL:

- Simpl-Open, el software de código abierto que alimenta los espacios de datos y otras iniciativas de federación de datos en nubes;
- Simpl-Labs, un entorno de demostración preinstalado en el que se podrá experimentar con el despliegue, mantenimiento y soporte del código abierto antes de desplegarlo para sus propias necesidades o evaluar su nivel de interoperabilidad de los espacios de datos más desarrollados;

[40] Véase su página web en Data Spaces Support Centre, disponible en https://dssc.eu/ [Última consulta: 15 de marzo de 2025].
[41] Véase *DSSC Delivery Plan - Summary of assets publication*, disponible *online* en https://dssc.eu/space/DDP/117211137/DSSC+Delivery+Plan+-+Summary+of+assets+publication
[42] Véase Simpl: Cloud-to-edge federations empowering EU data spaces, disponible *onine* en https://digital-strategy.ec.europa.eu/en/policies/simpl [Última consulta: 15 de marzo de 2025].

- Simpl-Open, que son entornos de producción personalizados para espacios de datos sectoriales (idiomas, administraciones públicas (contratación pública), Green Deal (comunidades inteligentes y Destination Earth), sanidad (eHealth secundaria), investigación e innovación), en los que la propia Comisión desempeña un papel activo en su gestión.

4.3. El European Data Innovation Board (EDIB)

El European Data Innovation Board (EDIB)[43] fue creado por la Commission Decision of 20.02.2023 setting up the European Data Innovation Board[44], siguiendo lo dispuesto por la Data Governance Act en su artículo 29(1)[45]. Lo constituye un grupo de expertos en las materias propias de la DGA, en particular la estandarización de datos y la interoperabilidad, que comprende representantes de los Estados miembros, el Consejo Europeo de Protección de Datos, el Supervisor Europeo de Protección de Datos, la Agencia de Ciberseguridad de la Unión Europea, el Representante para las PYME de la UE o un representante designado por la red de representantes para las PYME, y otros representantes de organismos pertinentes en sectores específicos y de organismos con conocimientos específicos[46].

El European Data Innovation Board (EDIB) tiene como misión fundamental asistir a la Comisión en la coordinación de las prácticas y políticas nacionales y en el uso intersectorial de los datos, pero sin influir en los trabajos de estandarización que se lleven a cabo en sectores o ámbitos específicos. Los trabajos de estandarización técnica pueden incluir (i) la identificación de prioridades para el desarrollo de normas; y (ii) el establecimiento y mantenimiento de un conjunto de normas técnicas y jurídicas para la transmisión de datos entre dos entornos de procesamiento que permita organizar espacios de datos sin recurrir a un intermediario. Sus funciones precisas se corresponden, en todo caso, con lo dispuesto en el artículo 30 de la LGD, que es la que estipulaba originalmente su creación, como hemos señalado ya anteriormente.

4.4. Otras iniciativas

Más allá de todo lo explicitado ya, conviene destacar que la UE está financiando numerosas iniciativas en el ámbito de los catorce sectores en los que se han dividido los espacios de datos. Una lista de iniciativas europeas comunes sobre el espacio de datos financiadas por la UE puede

[43] Consejo Europeo de Innovación de Datos
[44] Brussels, 20.2.2023 C(2023) 1074 final
[45] Véase también al respecto sus Considerandos 53 y 54.
[46] Commission Decision of 20.02.2023 setting up the European Data Innovation Board, Brussels, 20.2.2023 C(2023) 1074 final, Artículo 3.

hallarse en el Commission Staff Working Document on Common European Data Spaces, Brussels, 24.1.2024 SWD(2024) 21 final, Anexo I[47]. El Anexo II del mismo documento aporta una estimación del calendario de implementación de las iniciativas encaminadas a potenciar estos espacios.

5. El Espacio Europeo de Datos de Salud como ejemplo arquetípico de espacio de datos

En apartados anteriores hemos explicado la concepción de los espacios de datos articulada en torno al marco normativo general apenas descrito. Ahora bien, este escenario se concretará en una serie de medidas específicas encaminadas a regular cada espacio en concreto. De entre todas, ellas, el recientemente publicado Reglamento del Espacio Europeo de Datos de salud[48] merece especial consideración, en cuanto que constituye un ejemplo arquetípico de espacio de datos, figura a la que su propia redacción hace referencia. De hecho, su artículo 75.11 señala que "Los Estados miembros y la Comisión procurarán garantizar que DatosSalud@UE sea interoperable con otros espacios comunes europeos de datos pertinentes a que se refieren los Reglamentos (UE) 2022/868 y (UE) 2023/2854".

De ahí que en este último apartado vayamos a describir brevemente su funcionamiento, expresando sobre todo su principal diferencia con la norma general, la LGD, que estriba en el carácter público que presumiblemente adoptarán los organismos intermediarios creados por esta norma, esto es, los Organismos de Acceso. Con tal fin, nos centraremos especialmente en los actores que participan en la estructura, para luego describir brevemente el sistema de acceso a los datos. Finalmente, procederemos a ilustrar sus similitudes y diferencias con lo que dispone, en general, la LGD.

5.1. Los actores

El Reglamento del Espacio Europeo de Datos de salud se configura como un sistema complejo donde interactúan diversos actores, cada uno con un papel fundamental en la gestión y el uso de datos de salud. Algunos de ellos se corresponden con las categorías descritas en la LGD y otros claramente no. Esto se debe, indudablemente, a las características propias del sector sanitario. Los fundamentales, de entre todos ellos, son cinco: los tenedores de los datos, los usuarios de

[47] Véase Common European Data Spaces, disponible *online* en https://digital-strategy.ec.europa.eu/en/policies/data-spaces [Última consulta: 15 de marzo de 2025].

[48] 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. Publicado en el DOUE núm. 327, de 5 de marzo de 2025, pp. 1 – 96, disponible *online* en www.boe.es/buscar/doc.php?id=DOUE-L-2025-80382 [Última consulta: 15 de marzo de 2025].

datos, los organismos de acceso a los datos de salud, los intermediarios de datos y los participantes autorizados[49].

5.1.1. Tenedores de datos

En primer lugar, de acuerdo con el artículo 2.2 (t), el tenedor de datos de salud es:

> *"toda persona física o jurídica, autoridad pública, agencia u otro organismo del sector de la asistencia sanitaria o el asistencial, incluidos los servicios de reembolso cuando sea necesario, así como cualquier persona física o jurídica que desarrolle productos o servicios destinados al sector de la salud, el de la asistencia sanitaria o el asistencial, que desarrolle o cree aplicaciones de bienestar, que efectúe investigaciones científicas relacionadas con el sector de la asistencia sanitaria o el asistencial o que actúe como registro de mortalidad, así como las instituciones, órganos u organismos de la Unión, que tengan bien:*
>
> > *i) el derecho o la obligación, de conformidad con el Derecho de la Unión o nacional aplicable y en su calidad de responsable o corresponsable del tratamiento, de tratar datos de salud electrónicos personales para fines de prestación de asistencia sanitaria o fines asistenciales, o para fines de salud pública, reembolso, investigación, innovación, formulación de políticas, estadísticas oficiales o seguridad del paciente o para fines de regulación, o*
> >
> > *ii) la capacidad de poner a disposición datos de salud electrónicos no personales mediante el control del diseño técnico de un producto y de los servicios conexos, incluido mediante el registro, la entrega, la limitación del acceso o el intercambio de dichos datos;*

Se trata, por tanto, de una categoría amplísima, que incluye de hecho a todos aquellos agentes que operen en el sector de la salud bajo cuyo control se encuentran grandes bases de datos de salud o genéticos, excluidos, de acuerdo con el artículo 50.1 (b) los investigadores individuales, las personas físicas y las microempresas (tal y como se definen en el artículo 2, apartado 3, del anexo de la Recomendación 2003/361/EC de la Comisión de 6 de mayo de 2003 sobre la definición de microempresas, pequeñas y medianas empresas), salvo que los Estados miembros

[49] Véase al respecto: NAVAS NAVARRO, Susana, *Datos sanitarios electrónicos: el espacio europeo de datos sanitarios*, Reus, 2023; RECUERO, Mikel, «El Espacio Europeo de Datos de Salud: retos y oportunidades para la protección de datos de carácter personal», *Fodertics 10.0: estudios sobre derecho digital* / coord. por Irene González Pulido; Federico Bueno de Mata (aut.), Lorenzo Mateo Bujosa Vadell (pr.), 2022, ISBN 978-84-1369-452-8, págs. 389-402; SHABANI, Mahsa, «Will the European Health Data Space change data sharing rules?», *Science*, 375, 2022, p. 1357 y ss; Santa Slokenberga, Katharina Ó Cathaoir, Mahsa Shabani, *The European Health Data SpaceExamining A New Era in Data Protection,* Routledge, 2025.

decidan lo contrario a través de su normativa nacional (art. 50.2), en cuyo caso tendrán que notificar la aprobación de esta normativa, así como cualquier posible enmienda o regla derivada de ella que se apruebe posteriormente a la Comisión (art. 50.4).

En definitiva, serán aquellos responsables de gestionar y almacenar los grandes volúmenes de datos relacionados con la salud o datos genéticos. Esto incluye tanto la recopilación como el tratamiento inicial de dicha información. Los tenedores de datos tienen la responsabilidad de garantizar el cumplimiento de las normativas de protección de datos y están sujetos a las obligaciones establecidas en el artículo 60 del EEDS.

5.1.2. Usuarios de datos

Por otro lado, se encuentran los usuarios de datos. Un usuario de datos es, según el artículo 2.2 (u) *"una persona física o jurídica, incluidas las instituciones, órganos u organismos de la Unión, a la que se ha concedido acceso lícito a datos de salud electrónicos para uso secundario en virtud de un permiso de datos, una petición de datos de salud o una aprobación de acceso por parte de un participante autorizado en DatosSalud@UE".* Los datos pueden ser personales o no personales. Estos usuarios están autorizados para utilizar la información con fines comerciales o no comerciales, como investigación, innovación, desarrollo de nuevos tratamientos o elaboración de políticas de salud, como veremos más adelante.

Es importante subrayar que estos usuarios pueden ser personas o empresas radicadas en la UE o no, siempre que obtengan las autorizaciones administrativas que el mismo EEDS impone. Pueden ser entes públicos o empresas privadas, personas jurídicas o personas naturales, trabajando en su propio beneficio o por encargo de un tercero de carácter público, sin que todo ello implique diferencias relevantes, más allá de las que afectan a algunas de las finalidades previstas en el del EEDS, o las que afectan al derecho de autoexclusión.

Un ejemplo típico sería el de una empresa farmacéutica que solicita acceso a datos de salud electrónicos almacenados en hospitales de diferentes Estados miembros. Su propósito podría ser el de analizar datos de salud para desarrollar un nuevo tratamiento. Para ello, la empresa presentará una solicitud de acceso a los datos necesarios (ante el correspondiente organismo de acceso) mediante la infraestructura de DatosSalud@UE, y estos serán procesados y facilitados conforme a la normativa del EEDS.

5.1.3. Organismos de Acceso a los datos de salud

Entre estos dos primeros grupos se sitúan los Organismos de Acceso a los datos de salud (Oas), que desempeñan un papel crucial en la supervisión y facilitación del acceso a los datos

electrónicos de salud en los Estados miembros que dependan de ellos, así como en la consecución de una aplicación coherente del EEDS, por lo que se les impone el deber de cooperar entre sí y con la Comisión, así como, por lo que respecta a la protección de datos, con las autoridades de control pertinentes. Se trata, en suma, de una nueva figura que aparece para garantizar que el uso secundario de los datos se realice acorde al Reglamento, contribuyendo a la coherente aplicación del mismo y a la implementación de las garantías precisas para que el tratamiento de los datos para los fines previstos en el propio EEDS no se haga a costa de atentar contra los derechos e intereses de los ciudadanos. De hecho, entre sus objetivos se incluye el de garantizar la calidad y la ética en el tratamiento de datos, así como la promoción de buenas prácticas en el manejo de la información sanitaria. Con el fin de garantizar que actúan de manera coordinada, cada Estado miembro ha de designar a uno de ellos como coordinador, en caso de que haya más de uno, para las

Los artículos 55 y siguientes del Reglamento son los encargados de regular los OAs. Algunas de sus características principales están bien definidas ahí. Así, por ejemplo, el artículo 55 explicita que “Los Estados miembros designarán uno o varios organismos de acceso a datos de salud responsables de cumplir las funciones y obligaciones establecidas en los artículos 57, 58 y 59. Los Estados miembros podrán crear uno o varios nuevos organismos del sector público o recurrir a organismos del sector público existentes o a servicios internos de organismos del sector público que cumplan las condiciones establecidas en el presente artículo. Las funciones establecidas en el artículo 57 podrán repartirse entre diferentes organismos de acceso a datos de salud. Cuando un Estado miembro designe varios organismos de acceso a datos de salud, elegirá a uno de ellos para actuar como coordinador, con la responsabilidad de coordinar las funciones con los demás organismos de acceso a datos de salud, tanto en el territorio de ese Estado miembro como en los demás Estados miembros”. Por tanto, habrá al menos un Organismo de Acceso en cada Estado miembro, sin que se descarte que pueda haber más, y tendrán carácter de organismos públicos. Sus variadas funciones se hallan descritas en el artículo 57.1 del EEDS. Entre ellas destaca la de conceder o denegar los permisos de acceso a los datos a los usuarios de datos.

Los OAs son, en buena medida, la pieza clave de la arquitectura construida por el EEDS. Ellos actuarán como el punto de contacto o más bien de intermediación entre los usuarios o solicitantes de datos (investigadores, entidades públicas o privadas) y poseedores de bases de datos de salud electrónicos, los tenedores, siempre desde una posición de superioridad que les permitirá gobernar efectivamente todo el proceso, así como dar cuenta de sus resultados. Ahora bien, dicha intermediación incluirá capacidades que superan lo que habitualmente se asocia a este papel, ya que estos organismos podrán tratar las bases de datos con un alto grado de libertad, en función de lo que consideren más adecuado para los fines que un usuario pretenda conseguir, siempre dentro de lo que dispone el EEDS. En este sentido, los OAs no se corresponden con la figura de intermediario tal y como se halla descrita en la LGD, dado su

carácter de organismo administrativo y su posición jurídica de superioridad sobre los tenedores y usuarios de datos.

Aunque se trata de una nueva entidad, no es una figura muy novedosa, ya que en realidad es un cuerpo estrechamente relacionado con los Comités de Ética de la Investigación. La importancia estratégica de los Oas radica en la necesidad de garantizar la legalidad y la ética en el uso de datos, así como en la necesidad de crear un entorno confiable para el intercambio de información sanitaria. En síntesis, los Oas representan una interfaz crítica entre los tenedores de datos, los usuarios y el marco normativo del EEDS, asegurando que los datos de salud sean utilizados de manera eficiente, ética y segura.

5.1.4. Intermediarios de datos

Hay, finalmente, que hablar de una cuarta categoría de agentes, si bien de menor importancia que las tres anteriores: las entidades de intermediación de datos de salud, entendiéndose como tal las *"personas jurídicas capaces de tratar, poner a disposición, registrar, proporcionar, limitar el acceso e intercambiar datos de salud electrónicos para uso secundario proporcionados por los tenedores de datos".* (Considerando 59). Y es que el EEDS estipula que, con el fin de reducir la carga administrativa y a la luz de los principios de eficacia y eficiencia, los Estados miembros podrán decidir, mediante legislación nacional, que para determinadas categorías de tenedores de datos, sus obligaciones como tales sean desempeñadas por entidades de intermediación de datos de salud. En todo caso, esas entidades de intermediación de datos de salud realizan tareas diferentes a las de los servicios de intermediación de datos del Reglamento (UE) 2022/868.

Por tanto, las personas o entidades que generen o posean datos de salud (tenedores de datos) vean su carga administrativa reducida a través de la figura de los intermediarios de datos. En lugar de que cada tenedor de datos sea responsable de gestionar sus propios datos para su uso secundario, serán los intermediarios quienes se ocupen de dicha tarea. Su enfoque está centrado exclusivamente en datos de salud electrónicos. Sin embargo, el EEDS señala explícitamente que los intermediarios no podrán considerarse en ningún caso tenedores de datos de confianza.

5.1.5. Participantes autorizados

El EEDS no se construye sobre la nada. Existen ya infraestructuras de investigación establecidas en el ámbito de la UE, como los Consorcios de Infraestructuras de Investigación Europeas

(ERIC, por sus siglas en inglés) o de Infraestructuras Digitales Europeas (EDIC, por sus siglas en inglés) o el Foro Estratégico Europeo sobre Infraestructuras de Investigación (ESFRI, por sus siglas en inglés), o las infraestructuras federadas en el marco de la Nube Europea de la Ciencia Abierta (EOSC, por sus siglas en inglés). Todas ellas y otras estructuras similares, como el Sistema de Gestión Clínica de Pacientes u otros servicios o infraestructuras en los ámbitos de la salud, la asistencia o la seguridad social, etc., o los terceros países y las organizaciones internacionales que proporcionen a los usuarios de datos de salud situados en la Unión, en términos y condiciones equivalentes, acceso a los datos de salud electrónicos de que dispongan sus organismos de acceso a datos de salud, siempre que cumplan lo dispuesto en el capítulo V del Reglamento (UE) 2016/679 (art. 75) podrán ser participantes autorizados en DatosSalud@UE.

En muchos sentidos, los participantes autorizados serán equivalentes a los OAs. Entre otras cosas, recibirán las solicitudes de acceso a datos de salud cuando estas se refieran a datos que obren en poder de tenedores de datos de salud establecidos en más de un Estado miembro o de los participantes autorizados pertinentes en DatosSalud@UE a que se refiere el artículo 75, presentará una única solicitud de acceso a los datos de salud a través del organismo de acceso a datos de salud del Estado miembro donde esté situado el establecimiento principal del solicitante de datos de salud, a través del organismo de acceso a datos de salud del Estado miembro en el que esté establecido uno de esos tenedores de datos de salud o a través de los servicios prestados por la Comisión en DatosSalud@UE a que se refiere el artículo 75. La solicitud de acceso a datos de salud se transmitirá automáticamente a los participantes autorizados pertinentes en DatosSalud@UE y a los organismos de acceso a datos de salud de los Estados miembros en los que estén establecidos los tenedores de datos de salud identificados en la solicitud de acceso a datos de salud (artículo 67.3)[50].

5.2. El sistema de obtención de datos

Una vez que se conocen los actores que interactúan en el sistema, es relativamente fácil entender cómo funcionará el flujo de datos, al menos de manera simplificada[51]. El proceso comienza cuando un usuario de datos solicita un permiso a un OA para acceder a los datos que posee un tenedor de datos en concreto. El OA en cuestión puede aceptar o no la petición. Con tal fin, el OA tendrá que aseverar varias cosas, como que la finalidad del tratamiento se ajuste a

[50] La principal diferencia entre los OAs y los participantes autorizados, además del carácter de organismo administrativo que en el caso de los primeros será necesariamente ese y en el de los segundos, no, es que los participantes autorizados se enclavarán en la estructura de DatosSalud@UE. También, en que los OAs formarán parte del grupo rector DatosSalud@UE, mientras que los participantes autorizados sólo participarán con carácter de observadores (art. 95.5).

[51] Véase: DE MIGUEL BERIAIN, Iñigo, «El uso de datos de salud para investigación biomédica a la luz de la Propuesta del Parlamento Europeo y del Consejo sobre el Espacio Europeo de Datos Sanitarios», *Revista Jurídica de Castilla y León*, 60, 2023, pp. 7-35. ; RECUERO LINARES, Mikel «El uso secundario de datos de salud electrónicos: el futuro Reglamento del Espacio Europeo de Datos de Salud y su interacción con la protección de datos personales», *InDret* 2.2024, pp. 525-551.

las que el EEDS considera adecuadas, que no concurra ninguna de las prohibiciones al tratamiento del artículo 54 y que, además, se garantice la minimización en el tratamiento de los datos, lo que significa, entre otras cosas. Que sólo se tratarán datos anonimizados, salvo que el usuario justifique que para los fines previstos es preciso tratar datos personales, en cuyo caso serán siempre datos pseudonimizados.

En caso de que otorgue el permiso, el usuario podrá acceder a los datos en un entorno de tratamiento seguro, figura que se definía ya en la LGD como: *"el entorno físico o virtual y los medios organizativos para garantizar el cumplimiento del Derecho de la Unión, por lo que respecta a los derechos de los interesados, los derechos de propiedad intelectual y la confidencialidad comercial y estadística, la integridad y la accesibilidad, así como para garantizar el cumplimiento del Derecho nacional aplicable y permitir que la entidad encargada de proporcionar el entorno de tratamiento seguro determine y supervise todas las acciones de tratamiento, incluida la presentación, el almacenamiento, la descarga y la exportación de datos, así como el cálculo de datos derivados mediante algoritmos computacionales"*. El OA y el usuario se considerarán corresponsables del tratamiento de esos datos en el entorno seguro y al OA corresponderá garantizar que se respetan los derechos propios de las personas a las que corresponden los datos, entre otras cosas. Con tal fin, podrá almacenar los datos hasta el momento en que ya no sean necesarios para la investigación, sin que exceda de los diez años (existe posibilidad de prórroga debidamente justificada). Seis meses después de la expiración del permiso de datos, estos deberán suprimirse, de acuerdo al artículo 68.12 EEDS.

Si el usuario de datos considera que puede alcanzar los objetivos de su investigación a través de *una respuesta obtenida únicamente en formato estadístico anonimizado, podrá formular una petición de datos*. En tales casos, los organismos de acceso a datos de salud *no* responderán a una petición de datos en *ningún otro* formato y el usuario de datos de salud no tendrá acceso a los datos de salud electrónicos utilizados para proporcionar dicha respuesta. El artículo 69 del EEDS regula el procedimiento mediante el cual un solicitante de datos puede presentar una petición de datos de salud a los OAs. La respuesta será en *formato estadístico anonumizado,* como ya hemos apuntado, esto implica que el solicitante no tendrá acceso directo a los datos de salud electrónicos, sino únicamente a los resultados procesados en forma de estadísticas agregadas. Para que la solicitud sea válida, el solicitante debe proporcionar información detallada sobre su identidad, su actividad profesional y el propósito específico de la petición, asegurando que el uso propuesto se ajuste a los fines permitidos en el artículo 53 del EEDS (por ejemplo, investigación o salud pública). Además, la solicitud debe incluir una descripción del tipo de datos solicitados, el formato en el que se requiere la respuesta, el contenido estadístico esperado y las medidas adoptadas para evitar un uso indebido de los datos. Los OAs tienen un plazo de tres meses para evaluar la solicitud y, si es aceptada, deben proporcionar la respuesta en un máximo de seis meses desde su recepción. Durante este proceso, los OAs analizarán los riesgos asociados a la difusión de los datos, conforme al artículo 68.2, asegurando que la información proporcionada no comprometa la privacidad de los ciudadanos ni vulnere normativas de protección de datos, como el RGPD.

5.3. La Ley de Gobernanza de Datos y el EEDS

Como hemos apuntado anteriormente, el EEDS constituye en buena medida una norma que concreta lo dispuesto por la LGD, en general, para la gobernanza de la compartición de datos en el UE. De hecho, como ya hemos dicho la LGD establece el marco general para la intermediación de datos en la UE y proporciona un modelo normativo que fomenta la compartición de datos de forma segura, voluntaria y basada en la confianza. Siguiendo su mismo espíritu, el EEDS adopta varios de los principios fundamentales de la LGD y se postula como ejemplo arquetípico de espacio de datos. En este apartado analizaremos cómo encaja el EEDS en la estrategia europea de datos y cómo complementa a la LGD en el sector sanitario[52].

5.3.1. Similitudes

Al tratarse la LGD de una normativa marco en la que el EEDS se basa, sus similitudes son evidentes. En primer lugar, comparten una misma finalidad, ambas cuentan con el objetivo de facilitar el acceso a los datos. La motivación de ambas regulaciones se basa en permitir la reutilización de datos de forma controlada y con garantía, promoviendo la innovación y la investigación en la UE. Se busca desbloquear el potencial de los datos para el desarrollo de nuevas tecnologías.

En segundo lugar, ambas normas insisten en la necesidad de garantizar la interoperabilidad de los datos para que puedan ser utilizados entre distintos sectores y países de la UE. La LGD introduce requisitos generales para asegurar la compatibilidad de los espacios de datos, y el EEDS aplica estos principios al sector sanitario para permitir el acceso a la información clínica de manera estandarizada en toda Europa, si bien es cierto que muchas de sus previsiones deberán concretarse en los años posteriores a su publicación.

Por otro lado, uno de los principales aportes de la LGD al EEDS es la regulación de la intermediación de datos, es decir, la creación de entidades que faciliten el intercambio de información sin explotarla comercialmente. La LGD crea una infraestructura y establece un mecanismo de gobernanza de datos en la que el EEDS se inspira para adaptarse al sector sanitario. La intermediación de datos se hace en el EEDS mediante los Organismos de Acceso a los Datos de salud (OAs), que es una figura diseñada para garantizar que los datos se puedan tratar de manera controlada. De este modo, los OAs permiten reforzar la confianza en el ecosistema de datos, que es uno de los objetivos de la LGD. Y es que, como determinan Michelli et al, “este nuevo marco se ha desarrollado para tranquilizar a los interesados/titulares sobre

[52] KISELEVA, Anastasiya/DE HERT, Paul, «Creating a European Health Data Space: obstacles in four key legal areas», *European Pharmaceutical Law Review*, 5(1), 2021, p. 21 y ss.

cómo se tratarán sus datos"[53]. Los OAs, de hecho, desarrollan la función prevista para los intermediarios de datos, tal y como figuran descritos en la LED, generando un entorno seguro para la compartición de datos. De este modo se consigue conciliar la necesidad de tratar datos de salud para fines de investigación e innovación con la protección de los derechos e intereses de ciudadanos y pacientes.

5.3.2. Desviaciones del EEDS de la LGD

Para entender las esenciales diferencias entre las normas que ahora nos ocupan, convendría comenzar señalando que ambas regulaciones buscan un objetivo común, pero su ámbito de aplicación es distinto. La LGD es una norma trasversal aplicable a múltiples sectores como la industria, el transporte, la energía, etc. En cambio, como ya hemos mencionado, el EEDS es una norma centrada exclusivamente en los datos de salud y su reutilización dentro del sistema de salud europeo. En esta diferencia encuentran su razón de ser la mayoría de disparidades entre ambas normas. La naturaleza de los datos de salud, en cuanto que categorías especiales de datos según el artículo 9 del RGPD, requiere una mayor protección de privacidad y seguridad[54] en comparación con otros tipos de datos industriales o comerciales. Por ello, en el EEDS se opta por un enfoque más estricto, con un control directo del sector público sobre el acceso y la reutilización de la información.

Consecuentemente, en el Espacio Europeo de Datos de Salud, hay una mayor intervención de las Administraciones Públicas. Los OAs se han concebido de tal forma que difícilmente serán otra cosa que organismos administrativos, con independencia funcional y económica, a quienes competerá, entre otras, conceder el acceso a los datos de salud electrónicos mediante el otorgamiento de un permiso de acceso a datos y previa solicitud de acceso por un usuario de datos.[55]

Por otra parte, el acceso a los datos es también distinto, en el Espacio Europeo de Datos de Salud, ya que los datos de salud solo pueden ser utilizados en un entorno de tratamiento seguro, donde estos se procesan sin posibilidad de extracción no autorizada. Los OAs pueden rechazar solicitudes, auditar el uso de los datos y sancionar a quienes incumplan la normativa. Algo que no ocurre con la intermediación de datos, donde no hay restricciones estrictas sobre el entorno en el que se procesan los datos, sino que los intermediarios meramente se encargan de

[53] Micheli, M / Farrell, E / Carballa-Smichowski, B / Posada-Sanchez, M. /Signorelli, S / Vespe, M, *Mapping the landscape of data intermediaries— Emerging models for more inclusive data governance*, Publications Office of the European Union, Luxembourg, 2023, doi: 10.2760/261724, Disponible en https://publications.jrc.ec.europa.eu/repository/handle/JRC133988

[54] Véase Art. 9 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, a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos)

[55] Recuero, Mikel, «El uso secundario de datos de salud electrónicos: el futuro Reglamento del Espacio Europeo de Datos de Salud y su interacción con la protección de datos personales.», *InDret*, 2024, p.549 y ss.

proporcionar infraestructura y garantizar que las partes que comparten datos lo hagan bajo condiciones claras, pero no regulan activamente el acceso o el uso posterior de los datos.

Además, en la LGD, el intercambio de datos dependerá del tipo de datos que se trate y de quién los posea. En el EEDS hay un mayor grado de concreción sobre cómo funcionará el régimen de bases de legitimación del tratamiento. En principio, el consentimiento no es el mecanismo para el uso secundario de datos, sino que se parte de la base de que hay intereses que aconsejan promover el uso de los datos, intereses públicos, por lo que esta base de legitimación jugará un papel primordial. Esto no significa que la voluntad del ciudadano/paciente no tenga ningún peso. De hecho, el EEDS introduce el derecho de autoexclusión (opt out) como forma de preservar la autonomía individual. Se trata de un derecho de naturaleza peculiar, que faculta a las personas a optar por no participar en el régimen de utilización de datos para investigación o innovación, que se halla recogido en el artículo 71: "*Las personas físicas tendrán derecho de autoexclusión, en cualquier momento y sin necesidad de exponer los motivos, del tratamiento de los datos de salud electrónicos personales que les conciernan para uso secundario en el marco del presente Reglamento. El ejercicio de ese derecho será revocable*." Con todo, en algunas ocasiones y bajo ciertas condiciones es posible llegar a utilizar esos datos aun en contra de la voluntad de las personas a las que se refieren, cosa difícilmente imaginable en el caso del entorno de la LGD.

El enfoque del EEDS, en suma, es más intervencionista que el de la LGD y responde a la necesidad de garantizar un acceso amplio a los datos de salud para mejorar la investigación e innovación biosanitaria y la eficiencia de los sistemas sanitarios. La LGD busca crear un ecosistema de datos basado en la transparencia y la confianza, mientras que el EEDS prioriza el acceso amplio y regulado a los datos de salud, procurando que exista el menor número de barreras para fines como los del interés público. No obstante, la inclusión del derecho a la autoexclusión introduce una concesión a la defensa del interés particular frente al interés público. Habrá que ver, en todo caso, cómo se concreta en la práctica y cuáles son sus consecuencias finales.

En conclusión, observamos como el EEDS se erige como un desarrollo sectorial específico dentro del marco establecido por la LGD. Aunque ambas normativas comparten el objetivo de la reutilización de datos dentro de la Estrategia Europea de Datos, el EEDS introduce un modelo más restrictivo y regulado, con una mayor intervención de las Administraciones Públicas, debido a la sensibilidad de los datos de salud, en contraste con la mayor flexibilidad de la LGD en sectores menos críticos.

6. Conclusiones

Durante los últimos años, las instituciones europeas han realizado un considerable esfuerzo por producir unas normativas y crear unas instituciones capaces de asegurar el aprovechamiento del enorme volumen de datos personales disponibles para la investigación y la innovación científicas, siguiendo lo propuesto en la Estrategia Europea. La aprobación de la Directiva de datos abiertos y reutilización de la información del sector público o de la Ley de Gobernanza de Datos son excelentes ejemplos en este sentido. Tambien lo es, por supuesto, el desarrollo de una serie de organismos, estructuras y capacidades generales dedicadas a este fin como el Data Spaces Support Centre, Simpl: Smart Open-Source Middleware y el European Data Innovation Board (EDIB). Todo ello debería servir para ir creando los espacios de datos que, según la Estrategia mencionada, constituyen la espina dorsal del sistema.

A tenor de lo descrito en estas páginas, es posible concluir que el Reglamento Europeo Relativo al Espacio Europeo de Datos de Salud supone en buena medida la primera plasmación de un espacio de datos construido con una normativa propia, basada en las características del tipo de dato que se pretende regular. En este sentido, su principal aportación consiste en superar algunas de las deficiencias presentes en la aplicación práctica del Reglamento Europeo de Protección de Datos, sobre todo las relativas a la necesidad de contar con normativas específicas que avalen el tratamiento de datos de categorías especiales, como los datos de salud. Es sobradamente conocido en este sentido que muchos de los Estados miembros, como Alemania o Polonia no han resuelto adecuadamente la cuestión, recurriendo sistemáticamente al consentimiento como base de legitimación del tratamiento de estos datos, lo que causa graves disfunciones tanto a la hora de movilizar estos datos como en términos de armonización de bases de datos a nivel europeo.

La cuestión que queda ahora por resolver es si estas modificaciones normativas serán suficientes para lograr que, efectivamente, seamos capaces de aprovechar todo el potencial de los datos de salud. Otras, que ya introdujeron novedades, como el altruismo de datos que reguló la Ley de Gobernanza de Datos, han sido poco eficientes en este sentido. Nos tememos que las frecuentes indefiniciones en muchos de los aspectos de este nuevo Reglamento, como las que atañen a las tasas o el respecto a la propiedad intelectual puedan ser graves lastres en este sentido.

7. Referencias bibliográficas

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)

REGLAMENTO (UE) 2019/881 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 17 de abril de 2019 relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) nº 526/2013 («Reglamento sobre la Ciberseguridad»)

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

DIRECTIVA (UE) 2019/770 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 20 de mayo de 2019 relativa a determinados aspectos de los contratos de suministro de contenidos y servicios digitales

Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Una Estrategia Europea de Datos. COM(2020) 66 final

VCarvalho, G., Kazim, E. «Themes in data strategy: thematic analysis of 'A European Strategy for Data' (EC)». *AI Ethics* 2, 53–63 (2022), https://doi.org/10.1007/s43681-021-00102-y

Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Una Estrategia Europea de Datos. COM(2020) 66 final

Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Una Estrategia Europea de Datos. COM(2020) 66 final, Punto 5.D)

Commission Staff Working Document on Common European Data Spaces, Brussels, 24.1.2024 SWD(2024) 21 final. Disponible *online* en: https://digital-strategy.ec.europa.eu/en/policies/data-spaces

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)

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)

Micheli, M / Farrell, E / Carballa-Smichowski, B / Posada-Sanchez, M. /Signorelli, S / Vespe, *M*, *Mapping the landscape of data intermediaries— Emerging models for more inclusive data governance,* Publications Office of the European Union, Luxembourg, 2023, doi: 10.2760/261724, Disponble en https://publications.jrc.ec.europa.eu/repository/handle/JRC133988

Data Governance Act explained, disponible *online* en https://digital-strategy.ec.europa.eu/en/policies/data-governance-act-explained [Última consulta: 15 de marzo de 2025]

Considerando 11 de la DGA

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)

Eckardt, M., & Kerber, W. (2024). «Property rights theory, bundles of rights on IoT data, and the EU Data Act». *European Journal of Law and Economics*, *57*(1), pp. 113-143.

Drexl, J., et al. (2022). Position statement of the Max Planck institute for innovation and competition of 25 May 2022 on the Commission's Proposal of 23 February 2022 for a regulation on harmonized rules on fair access to and use of data (Data Act) (May 25, 2022). Max Planck institute for innovation & competition research paper No. 22–05. Retrieved February 26, 2022 from https://ssrn.com/abstract=4136484, https://doi.org/ 10.2139/ssrn.4136484

Kerber, W. (2023b). «Data Act and competition: An ambivalent relationship», *Concurrences* No.1–2023, pp. 30–36.

Kerber, W, «Governance of IoT data: why the EU Data Act will not fulfill its objective». *GRUR International,* 72(2), pp. 120-135.

Kerber, «Data-sharing in IoT ecosystems and competition law: The example of connected cars». *Journal of Competition Law & Economics, 15*, pp. 381–426.

Eckardt, M., & Kerber, W, «Property rights theory, bundles of rights on IoT data, and the EU Data Act». *European Journal of Law and Economics*, *57*(1), pp. 113-143.

Leistner, M./ Antoine, L. (2022). «IPR and the use of open data and data sharing initiatives by public and private actors, study commissioned by the European Parliament's Policy Department for citizens' rights and constitutional affairs at the request of the Committee on Legal Affairs». Disponible en: https://doi.org/10.2139/ssrn.4125503

Atik, C,«Towards comprehensive agricultural data governance: Moving beyond the "data ownership" debate». *IIC-International Review of Intellectual Property and Competition Law, 53*, p. 701 y ss.

Directiva 2003/98/ CE del Parlamento Europeo y del Consejo de 17 de noviembre de 2003, relativa a la reutilización de la información del sector público.

Considerando 3 de la 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.

Support Centre for Data Sharing (SCDS), *Analytical report on EU law applicable to sharing of non-personal data Support Centre for data sharing,* 2020, pp. 43-62. Disponible en: https://data.europa.eu/sites/default/files/course/EU%20law%20applicable%20to%20sharing%20of%20non-personal%20data.pdf

Considerando 23 de la Directiva (UE) 2019/1024.

Support Centre for Data Sharing (SCDS), *Analytical report on EU law applicable to sharing of non-personal data Support Centre for data sharing*, 2020, pp. 43-62. Disponible *online* en: https://data.europa.eu/sites/default/files/course/EU%20law%20applicable%20to%20sharing%20of%20non-personal%20data.pdf

Commission Staff Working Document on Common European Data Spaces, Brussels, 24.1.2024 SWD(2024) 21 final, p. 11.

Data Spaces Support Centre, disponible en https://dssc.eu/ [Última consulta: 15 de marzo de 2025].

DSSC Delivery Plan - Summary of assets publication, disponible *online* en https://dssc.eu/space/DDP/117211137/DSSC+Delivery+Plan+-+Summary+of+assets+publication

Simpl: Cloud-to-edge federations empowering EU data spaces, disponible *onine* en https://digital-strategy.ec.europa.eu/en/policies/simpl [Última consulta: 15 de marzo de 2025].

Commission Decision of 20.02.2023 setting up the European Data Innovation Board, Brussels, 20.2.2023 C(2023) 1074 final, Artículo 3.

Common European Data Spaces, disponible online en https://digital-strategy.ec.europa.eu/en/policies/data-spaces [Última consulta: 15 de marzo de 2025].

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. Publicado en el DOUE núm. 327, de 5 de marzo de 2025, pp. 1 – 96, disponible *online* en www.boe.es/buscar/doc.php?id=DOUE-L-2025-80382 [Última consulta: 15 de marzo de 2025].

NAVAS NAVARRO, Susana, *Datos sanitarios electrónicos: el espacio europeo de datos sanitarios*, Reus, 2023;

RECUERO, Mikel, «El Espacio Europeo de Datos de Salud: retos y oportunidades para la protección de datos de carácter personal», *Fodertics 10.0: estudios sobre derecho digital* / coord. por Irene González Pulido; Federico Bueno de Mata (aut.), Lorenzo Mateo Bujosa Vadell (pr.), 2022, ISBN 978-84-1369-452-8, págs. 389-402;

SHABANI, Mahsa, «Will the European Health Data Space change data sharing rules?», *Science*, 375, 2022, p. 1357 y ss;

Santa Slokenberga, Katharina Ó Cathaoir, Mahsa Shabani, *The European Health Data SpaceExamining A New Era in Data Protection,* Routledge, 2025.

DE MIGUEL BERIAIN, Iñigo, «El uso de datos de salud para investigación biomédica a la luz de la Propuesta del Parlamento Europeo y del Consejo sobre el Espacio Europeo de Datos Sanitarios», *Revista Jurídica de Castilla y León*, 60, 2023, pp. 7-35. ; RECUERO LINARES, Mikel «El uso secundario de datos de salud electrónicos: el futuro Reglamento del Espacio Europeo de Datos de Salud y su interacción con la protección de datos personales», *InDret* 2.2024, pp. 525-551.

KISELEVA, Anastasiya / DE HERT, Paul, «Creating a European Health Data Space: obstacles in four key legal areas», *European Pharmaceutical Law Review*, 5(1), 2021, p. 21 y ss.

Art. 9 REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016, por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos)