

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

Sumario

-
La creación del Espacio Europeo de Datos de Salud por medio de la aprobación de su correspondiente Reglamento (REEDS) pretende erigirse como un importante hito para superar la fragmentación normativa existente, establecer mecanismos de gobernanza comunes y, en suma, impulsar la reutilización de datos de salud en beneficio de la sociedad y del interés general. El presente artículo tiene por objeto examinar el régimen propuesto para el uso secundario de datos de salud electrónicos, sus carencias y virtudes y su compleja integración e interacción con la normativa europea de protección de datos de carácter personal, en particular, el Reglamento General de Protección de Datos (RGPD).

Abstract

-
The setting of the European Health Data Space through the adoption of its corresponding Regulation (REHDS) represents a major milestone to overcome persisting regulatory fragmentation, to establish shared governance tools and, ultimately, to boost health data re-use for the common good. This paper aims to analyse the proposed regime for secondary uses of electronic health data, addressing its complex interplay with European data protection laws, notably, the General Data Protection Regulation (GDPR).

Title: *Secondary Use of Electronic Health Data: The Future Regulation on the European Health Data Space and its Interplay with Data Protection Law*

-
Palabras clave: usos secundarios, tratamiento ulterior, espacio europeo de datos, datos de salud, datos personales, datos sensibles, protección de datos.

Keywords: *Secondary Uses, Further Processing, European Data Space, Health Data, Personal Data, Sensitive Data, Data Protection*

-
DOI: 10.31009/InDret.2024.i2.13

2.2024

Recepción
05/01/2024

-
Aceptación
13/02/2024

Índice

-

- 1. Introducción y antecedentes**
- 2. Datos de salud electrónicos personales y usos secundarios: interacciones y asimetrías entre el Reglamento General de Protección de Datos (RGPD) y el futuro Reglamento del Espacio Europeo de Datos de Salud (REEDS)**
 - 2.1. Datos de salud electrónicos: ¿una doble vis expansiva?
 - 2.2. Uso secundario versus tratamiento ulterior de datos personales
- 3. Usos secundarios permitidos y usos secundarios prohibidos**
 - 3.1. Usos secundarios permitidos (art. 34): especial alusión a la investigación científica y la Inteligencia Artificial
 - 3.2. Usos secundarios prohibidos (art. 35)
- 4. Componentes y actores principales del Espacio Europeo de Datos de Salud**
 - 4.1. Titulares de datos
 - 4.2. Usuarios de datos
 - 4.3. Organismos de acceso a datos
 - 4.4. HealthData@EU
- 5. Condiciones y procedimientos para el acceso a datos de salud electrónicos en el Espacio Europeo de Datos de Salud**
 - 5.1. Procedimiento ordinario
 - 5.2. Procedimiento simplificado
- 6. Conclusiones**
- 7. Bibliografía**

-

Este trabajo se publica con una licencia Creative Commons Reconocimiento-
No Comercial 4.0 Internacional 

1. Introducción y antecedentes*

El 19 de febrero de 2020 la Comisión Europea hacía pública la Comunicación «Una Estrategia Europea de Datos», en la que esbozaba las líneas maestras de una serie de medidas políticas, legislativas, técnicas y presupuestarias encaminadas a desarrollar el potencial de los datos para la economía y la sociedad¹; lo que no se habría producido dada la persistencia de determinados problemas fácticos, jurídicos, económicos, tecnológicos y sociales². En dicho documento se propuso una acción conjunta de la Unión estructurada en cuatro pilares fundamentales:

i) La implementación de un marco común de gobernanza para el acceso y la reutilización de datos. Esto incluye, por un lado, medidas legislativas generales tales como la aprobación del Reglamento de Gobernanza Europea de Datos³. Por otro, el impulso de normas sectoriales, como es el caso de la Propuesta de Reglamento sobre el Espacio Europeo de Datos Sanitarios (en lo sucesivo, REEDS)⁴ que será objeto de análisis en el presente artículo.

ii) El desarrollo de capacidades e infraestructuras interoperables para el almacenamiento y el tratamiento de datos en el conjunto de la Unión Europea.

iii) El empoderamiento y la educación de la ciudadanía con respecto a sus datos personales, facultando un mayor control mediante el apuntalamiento de sus derechos de acceso y de portabilidad.

iv) La creación de un total de nueve espacios comunes europeos de datos en sectores estratégicos y en ámbitos de interés público. Desde un punto de vista técnico, un *espacio de datos* es una infraestructura federada y abierta para el acceso a datos, basada en una gobernanza, políticas,

* Autor/a de contacto: Mikel Recuero (mikel.recuero@ehu.eus). Este artículo se integra en el marco del proyecto de investigación «GODAS: Gobernanza de los usos secundarios de datos de salud y genéticos en espacios compartidos», PID2022-137140OB-I00, cofinanciado por el MCIN/AEI/10.13039/501100011033/FEDER. Asimismo, se ha desarrollado en el curso del proyecto «EuCanImage: A European Cancer Image Platform Linked to Biological and Health Data for Next-Generation Artificial Intelligence and Precision Medicine in Oncology», financiado por el Programa Horizonte 2020 de la Comisión Europea (European Union's Horizon 2020 Research and Innovation Programme, Grant Agreement No 952103). El autor quiere agradecer a las personas que componen los equipos de investigación de ambos proyectos todo su apoyo y las estimulantes discusiones que han precedido a la presente publicación.

¹ 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». Bruselas, 19.2.2020, COM(2020) 66 final.

² Un análisis multidisciplinar de los referidos problemas y barreras ha sido encomendado a la acción conjunta *Towards European Health Data Space* («TEHDAS»). Cabe citar, a tales efectos, sus informes: *Report on secondary use of health data through European case studies*, de 28 de febrero de 2022; *Summary of results and case studies on barrier to cross-border sharing of health data for secondary use*, de 28 de septiembre de 2021. Igualmente, resultan de mención obligatoria a estos efectos los estudios preliminares acometidos, entre otras, por: ALKORTA IDIAKEZ, *El Espacio Europeo de Datos Sanitarios: Nuevos enfoques para la protección e intercambio de datos sanitarios*, 2022 y NAVAS NAVARRO, *Datos sanitarios electrónicos: el espacio europeo de datos sanitarios*, 2023.

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 (RGED). OJ L 152, 3.6.2022, pp. 1–44.

⁴ Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el Espacio Europeo de Datos Sanitarios (REEDS). Estrasburgo, 3.5.2022, COM(2022) 197 final.

reglas y estándares que definen un marco de confianza para todos los intervinientes⁵. A grandes rasgos, un *dataspace* tiene por objeto proporcionar una funcionalidad básica común para un conjunto de fuentes de datos, con independencia de su formato y ubicación, permitiendo a tales fuentes y repositorios establecer relaciones entre sí respetando la autonomía y las facultades de control de cada participante sobre sus conjuntos de datos⁶.

Así, sobre la base de los citados ejes de acción se produce el impulso del llamado *Espacio Europeo de Datos de Salud* (en adelante, EEDS) que, además, ha sido el primero de los nueve previstos en ver la luz en forma de propuesta de Reglamento. Con toda probabilidad, ello se debe al advenimiento de la pandemia de COVID-19 poco tiempo después de la publicación de la meritada Estrategia que, por desgracia, terminó por refrendar su necesidad y prioridad⁷. Representa, en suma, una oportunidad formidable para abordar la fragmentación normativa persistente, establecer mecanismos de gobernanza comunes frente a la disparidad de sistemas que se han venido adoptando por cada Estado miembro y, en última instancia, apostar decididamente por una acción legislativa que impulse la reutilización de datos en beneficio de la sociedad y del interés general.

La primera versión de la Propuesta de REEDS se publica el 3 de mayo de 2022, encontrándose en el momento en que se escriben estas líneas en pleno proceso de discusión y negociación, con sendas propuestas de reforma del texto ya demandadas por el Parlamento Europeo⁸. Se trata de un instrumento de gran complejidad por cuanto ha de coexistir e interactuar con una miríada de normas ya vigentes o en desarrollo, debiendo aplicarse tanto a los datos personales como a los no personales y, finalmente, regulando una pluralidad de cuestiones interdisciplinarias. Es más, en relación con esto último, la Propuesta se divide en tres partes con objetivos diferenciados⁹:

i) Una primera parte cuyo objeto es la mejora del acceso de las personas físicas a sus datos de salud electrónicos y el control de dichos datos en el contexto de la asistencia sanitaria (uso primario). Capítulo II, arts. 3 a 13 de la Propuesta de REEDS.

⁵ AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, *Aproximación a los Espacios de Datos desde la perspectiva del RGPD*, 2023.

⁶ FRANKLIN, et al. «From databases to dataspace: A new abstraction for information management», *SIGMOND Record*, 34, n.º 4, 2005, p. 28. Entre los componentes esenciales de un espacio de datos habitualmente encontraremos: i) un catálogo de datos, que servirá como inventario de recursos con la información básica de cada uno de ellos; ii) un módulo de búsqueda y consulta; iii) componentes para el descubrimiento de conjuntos de datos relevantes y el establecimiento de relaciones entre los participantes; y iv) una infraestructura común para apoyar a aquellos participantes que carezcan de la suya propia o cuyas capacidades de computación sean insuficientes.

⁷ Así lo evidencian los Considerandos 2º y 3º de la Propuesta de REEDS que, respectivamente, destacan que la crisis de la COVID-19 sirvió para poner de relieve «la necesidad de tener un acceso oportuno a datos sanitarios electrónicos para la preparación y respuesta ante las amenazas para la salud» y, «de compartir datos sanitarios electrónicos que sean fáciles de encontrar, accesibles, interoperables y reutilizables».

⁸ PARLAMENTO EUROPEO (Committee on the Environment, Public Health and Food Safety & Committee on Civil Liberties, Justice and Home Affairs), *Draft Report on the proposal for a Regulation on the European Health Data Space*, 2022/0140(COD) 10/02/2023. Se hará referencia posteriormente a algunas de las reformas propuestas.

⁹ Véase Considerando 1 y art. 1 de la Propuesta de REEDS. La intervención legislativa de la UE se sustenta en el art. 114 del TFUE (mejora del funcionamiento del mercado interior, en particular, la garantía de un nivel de protección elevado de la salud humana) y el art. 16 del TFUE (protección de datos de carácter personal).

ii) Una segunda destinada al establecimiento de un marco jurídico uniforme en lo que respecta al desarrollo, la comercialización y el uso de sistemas de Historiales Médicos Electrónicos y aplicaciones sobre bienestar. Capítulo III, arts. 14 a 32 de la Propuesta de REEDS.

iii) Una última que persigue impulsar la reutilización de los datos de salud electrónicos para otros fines que beneficien a la sociedad, tales como la investigación, la innovación, la formulación de políticas, la seguridad de los pacientes, la medicina personalizada o las estadísticas oficiales (uso secundario). Capítulo IV, arts. 33-58.

En el presente artículo nos limitaremos a abordar, pues, esta última parte de la Propuesta, relativa a los usos secundarios de datos de salud electrónicos, con especial atención a aquellos de carácter personal. Para ello, primeramente, se analizarán las asimetrías e interacciones entre algunos de los conceptos esenciales de la Propuesta de REEDS y los correspondientes del Reglamento General de Protección de Datos (en lo sucesivo, RGPD)¹⁰ (*2. Datos de salud electrónicos personales y usos secundarios: interacciones y asimetrías entre el Reglamento General de Protección de Datos y el futuro Reglamento del Espacio Europeo de Datos de Salud*). Seguidamente, se llevará a cabo una lectura crítica de los usos secundarios permitidos y prohibidos en virtud de la Propuesta, con especial atención a la investigación científica y la Inteligencia Artificial (*3. Usos secundarios permitidos y usos secundarios prohibidos*). Tras ello, se presentarán los actores principales del REEDS en lo que a la infraestructura para el uso secundario de datos se refiere, examinando su encaje con los instrumentos jurídicos precedentes y, en particular, con la normativa de protección de datos personales (*4. Componentes y actores principales del Espacio Europeo de Datos de Salud*). Por último, ahondaremos en las condiciones y procedimientos sobre los cuales se sustanciará el acceso a datos de salud electrónicos para usos secundarios en el seno del meritado Espacio (*5. Condiciones y procedimientos para el acceso a datos de salud electrónicos en el Espacio Europeo de Datos de Salud*). Para finalizar, en el apartado de conclusiones (*6. Conclusiones*), se revisitarán las anteriores cuestiones con el fin de sintetizar las virtudes y carencias de la Propuesta y su eventual integración e interacción con la compleja lógica sistemática de la normativa europea de protección de datos de carácter personal.

2. Datos de salud electrónicos personales y usos secundarios: interacciones y asimetrías entre el Reglamento General de Protección de Datos (RGPD) y el futuro Reglamento del Espacio Europeo de Datos de Salud (REEDS)

Como se anticipaba, si bien el análisis de la Propuesta de REEDS puede acometerse desde una óptica diversa, los mayores retos para la protección de datos de carácter personal se plantean en lo que a los usos secundarios de los datos de salud electrónicos se refiere¹¹, verbigracia, por lo

¹⁰ 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 (RGPD). *DOUE L 119, 4.5.2016, p. 1-88*.

¹¹ Lo que no quiere decir, por supuesto, que el derecho fundamental a la protección de datos personales sea necesariamente (ni el único ni el principal) cuya afectación pueda llegar a producirse como consecuencia de los usos secundarios de datos de salud electrónicos. A tales efectos, cabe recordar que las informaciones relativas al estado de salud de una persona forman parte de la esfera más íntima y personal de un individuo, conformando un auténtico punto de contacto entre los derechos fundamentales a la protección de datos personales y el derecho a la intimidad o la vida privada, tal y como viene proclamando el Tribunal Europeo de Derechos Humanos. Así, si bien la protección de datos no deja de jugar un papel fundamental, las informaciones médicas o relativas a la salud de las personas «no son menos importantes para el derecho a la vida privada y familiar» habida cuenta de que su

dispuesto en el Capítulo IV (arts. 33 a 58) del texto. Es más, en su momento ya anticipábamos —cuando la Propuesta se hallaba en una fase todavía embrionaria— que sus interacciones y desavenencias con la normativa de protección de datos y, máxime, el RGPD, serían objeto de un sinnúmero de discusiones legislativas y académicas¹². No es para menos, pues ambas normas habrán de compartir, efectivamente, no solo una pluralidad de componentes y definiciones, también, un ámbito de aplicación parcialmente coincidente.

Esto no quiere decir, a nuestro juicio, que el REEDS aspire a ocupar una posición de *lex specialis* con respecto al RGPD: se trata, más bien, de dos instrumentos complementarios que han de encajar y convivir mutuamente en el (cada vez mayor) acervo de instrumentos directa o indirectamente relevantes para la protección de datos de carácter personal a nivel nacional y europeo. Por ello, en este afán de coexistencia los solapamientos y las remisiones normativas cruzadas no solo parecen inevitables, sino que, muy probablemente, deberán formar parte de la práctica cotidiana de todo intérprete y operador jurídico. A fin de arrojar algo de luz creemos conveniente destacar dos previsible fricciones interpretativas y aplicativas que habrán de resolverse antes incluso de acometer cualquier examen pormenorizado del texto del futuro REEDS. A saber, en primer lugar, la interacción del concepto de «datos de salud electrónicos» acuñado por la Propuesta con la noción de «datos relativos a la salud» acogida por el RGPD y, en su caso, si la primera encarna o no un alcance expansivo. En segundo lugar, la compatibilidad entre el «uso secundario de datos» abanderado por la Propuesta y el «tratamiento ulterior de datos personales» del que se ocupa el RGPD que, como veremos, generará importantes disfunciones prácticas al no tratarse de figuras absolutamente equiparables. Esclarecidas ambas cuestiones, nos ocuparemos de un análisis más detallado del texto de la Propuesta.

2.1. Datos de salud electrónicos: ¿una doble vis expansiva?

El concepto de «datos de salud electrónicos» y la definición que la Propuesta de REEDS le atribuye consolidan, a nuestro parecer, una clara tendencia expansiva desde una doble perspectiva: i) se extiende tanto a los datos electrónicos personales como a los no personales; y ii) es sustancialmente más amplia y comprehensiva que aquella de «datos relativos a la salud» que venía empleándose por el RGPD.

Por lo que se refiere a la primera cuestión, la propia Propuesta hace alusión explícita a un fenómeno que viene produciéndose sistemáticamente en el seno de la tradicional dicotomía entre el dato personal y el no personal: las crecientes dificultades para llevar a cabo una anonimización efectiva en el sentido del RGPD y, en esencia, para trazar una clara línea divisoria entre aquellos tratamientos de datos a los que el Reglamento habrá de aplicarse y aquellos que debieran quedar excluidos de su ámbito; especialmente, a la luz de los avances técnicos (v.g. Big Data, supercomputación, Inteligencia Artificial) y científicos (v.g. la prominencia de las ciencias

difusión «puede afectar dramáticamente a su vida privada y familiar o a su situación social o de empleo, exponiendo a la persona al oprobio y al ostracismo». Entre otras y por todas: STEDH, 22009/93 de 25 de febrero de 1997, Asunto Z v. Finlandia, §96). A lo que habría de adicionarse el potencial riesgo de estigmatización, discriminación o el menoscabo del libre desarrollo de la personalidad, tal y como ha admitido nuestro Tribunal Constitucional en acogimiento de la anterior línea jurisprudencial [STC (Sala Primera) 70/2009, de 23 de marzo de 2009, BOE núm. 102, de 27 de abril de 2009].

¹² RECUERO, «El Espacio Europeo de Datos de Salud: retos y oportunidades para la protección de datos de carácter personal», en BUENO DE MATA (dir.) / GONZÁLEZ PULIDO (coord.), *Fodertics 10.0: estudios sobre derecho digital*, Comares, Granada, 2022, p. 389.

-ómicas)¹³. Como consecuencia de ello, en aras de evitar que la posible materialización de los riesgos de reidentificación se traduzcan en un menoscabo del nivel de protección de los derechos y libertades de las personas físicas o en una quiebra de confianza en los mecanismos introducidos por el REEDS, la reacción legislativa ha sido la de extender el alcance de la Propuesta a todos los «datos de salud electrónicos», abarcando con ello tanto los datos personales como los no personales¹⁴. Ello tiende a afianzar la tendencia expansiva señalada en el sentido de que la exponencial indiferenciación entre datos personales y no personales se aborda en el plano normativo por medio de la ampliación del ámbito de aplicación de tales instrumentos¹⁵. Por otro lado, confirma el viraje hacia un modelo finalista en términos de la sensibilidad de los datos en tanto en cuanto pasan a autorizarse determinadas actividades o conjunto de actividades de tratamiento por razón de sus usos o finalidades, más allá de las clásicas prohibiciones por razón de la naturaleza o sensibilidad intrínsecas de los datos¹⁶. Finalmente, ello podría tener efectos asimismo significativos en la regulación aplicable a los datos de las personas fallecidas, que pasarían a tratarse como cualquier otro dato en el contexto del Espacio¹⁷.

La segunda desviación expansiva de la Propuesta de REEDS con respecto a lo dispuesto por el RGPD se refiere propiamente a la noción de «datos de salud electrónicos personales», que queda definida como «los datos relativos a la salud y los datos genéticos, tal como se definen en el Reglamento (UE) 2016/679, así como los datos relativos a factores determinantes de la salud, o los datos tratados en relación con la prestación de servicios sanitarios, que se traten en formato

¹³ Ilustrativo resulta, a este respecto, lo dispuesto por el Considerando 64 de la Propuesta: «Determinadas categorías de datos sanitarios electrónicos pueden seguir siendo especialmente sensibles incluso cuando estén en formato anonimizado y, por tanto, no sean personales (...). Incluso cuando se utilizan las técnicas de anonimización más avanzadas, sigue existiendo un riesgo residual de que pueda conseguirse la desanonimización. Esto puede afectar a diferentes tipos de datos sanitarios, lo que dependerá del nivel de granularidad y de descripción de las características de los interesados, o del número de personas afectadas. Y también puede afectar, por ejemplo, a los datos incluidos en historiales médicos electrónicos, registros de enfermedades, biobancos, datos generados por personas, etc., en los que las características de identificación son más amplias y en los que, en combinación con otra información (por ejemplo, en zonas geográficas muy pequeñas) o a través de la utilización de métodos tecnológicos que no estaban disponibles en el momento de la anonimización, se puede producir la desanonimización de los interesados utilizando medios que vayan más allá de aquellos cuya utilización era razonablemente previsible».

¹⁴ Véase la definición de «datos sanitarios electrónicos» del art. 2.2, letra c) de la Propuesta de REEDS: «los datos sanitarios electrónicos personales o no personales».

¹⁵ Decisión laudable en opinión de la AEDS, en la medida en que contribuye a un marco legal que «no se asiente nuevamente en un modelo dicotómico de anonimización o consentimiento, permitiendo el uso secundario de datos seudonimizados cuando ello sea lo más adecuado y necesario para el buen fin de la investigación». Vid. a este respecto: ASOCIACIÓN ESPAÑOLA DE DERECHO SANITARIO, *Recomendaciones sobre el nuevo Espacio Europeo de Datos de Salud*, recomendación núm. 6.

¹⁶ A este respecto constituye obra de referencia: JOVE VILLARES, *La protección de lo sensible, o cuando la naturaleza del dato no lo es todo*, 2023. Así pues, el modelo vigente se aproximaría a uno «contextual en naturaleza» en que, aun partiendo de la naturaleza sensible de la información como premisa, tal consideración habría de llevarse a cabo en última instancia en atención a los factores contextuales del tratamiento junto con la finalidad pretendida por el responsable del tratamiento. Vid. también, en este mismo sentido: NICOLÁS, Pilar, «El concepto de dato médico y genético», en RIPOL CARULLA (ed.) / BACARIA MARTRUS (coord.), *Estudios de protección de datos de carácter personal en el ámbito de la salud*, Marcial Pons, Barcelona, 2006, pp. 77 ss.; y QUINN/MALGIERI, «The Difficulty of Defining Sensitive Data – The Concept of Sensitive Data in the EU Data Protection Framework», *German Law Journal*, 22(8), 2022, pp. 1583 ss.

¹⁷ DE MIGUEL BERIAIN, «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, p. 7.

electrónico»¹⁸. Esta no es, ni mucho menos, la única disposición del texto que instila la enorme amplitud conceptual atribuible a la expresión. El origen o fuente de los datos puede ser diverso y no se circunscribe a los contextos puramente médicos, sanitarios o asistenciales¹⁹. Asimismo, la Propuesta enumera una serie de «categorías mínimas de datos electrónicos para uso secundario» que comprende un nada desdeñable listado abierto de quince categorías diferentes y que deben ser «lo suficientemente amplias y flexibles para responder a la evolución de las necesidades de los usuarios de los datos»²⁰. Este catálogo incluye, además de los datos propiamente médicos y/o sanitarios (v.g. historias clínicas, datos administrativos y de facturación, etc.), entre otros: datos sobre determinantes sociales, ambientales y de comportamiento relacionados con la salud; datos genómicos sobre patógenos relevantes para la salud humana; datos genéticos, genómicos y proteómicos humanos; datos procedentes de registros, ensayos clínicos, biobancos y bases de datos; y datos relativos al estilo de vida, el bienestar y el comportamiento relacionados con la salud, incluyendo aquellos recogidos por aplicaciones sobre bienestar. La única acotación apreciable parece referirse al formato de los datos en cuestión: deberán ser electrónicos, lo que excluirá, en principio, aquellos que figuren o se traten manualmente o por otros procedimientos o medios que no sean electrónicos (v.g. en ficheros físicos o en papel sin digitalizar).

Todo lo anterior denota que el ámbito conceptual atribuible a los «datos de salud electrónicos personales» es más extenso, si cabe, que la noción de «datos relativos a la salud» empleada por el RGPD²¹. Cabe recordar que esta última goza, ya de por sí, de un inusitado carácter abierto y expansivo en aras de capturar normativamente una concepción de salud holística y omnicompreensiva que desdibuja las líneas entre medicina, bienestar y estilo de vida²².

¹⁸ Art. 2.2, letra a) de la Propuesta de REEDS. El Considerando 5 provee un mayor desarrollo de esta definición: «Estos datos sanitarios electrónicos personales podrían incluir datos personales relacionados con la salud física o mental de las personas físicas, incluido el uso de los servicios de asistencia sanitaria, que revelen información sobre su estado de salud, y datos personales sobre las características genéticas heredadas o adquiridas de las personas físicas, que proporcionen información única sobre la fisiología o la salud de dicha persona física y que resulten, en particular, del análisis de una muestra biológica de la persona física en cuestión, así como datos sobre factores determinantes de la salud, como los conductuales, los medioambientales, las influencias físicas, la atención médica y los factores sociales o educativos». Tal ha sido la desviación con respecto a la noción dada por el RGPD que el Comité Europeo de Protección de Datos (CEPD) y el Supervisor Europeo de Protección de Datos (SEPD) han sugerido su supresión o reforma. Vid. a este respecto: Dictamen Conjunto núm. 2/2022 del CEPD y el SEPD sobre la Propuesta de Reglamento del Espacio Europeo de Datos Sanitarios, p. 13. En idénticos términos se ha pronunciado la AEDS, *Recomendaciones sobre el nuevo Espacio Europeo de Datos de Salud*, Rec. 2º.

¹⁹ Así lo disponen el Considerando 38 y el art. 33.3, que reza como sigue: «Los datos sanitarios electrónicos a que se refiere el apartado 1 abarcarán los datos tratados para la prestación de servicios sanitarios o asistenciales o para la salud pública, la investigación, la innovación, la elaboración de políticas, las estadísticas oficiales, la seguridad de los pacientes o con fines reglamentarios, recogidos por entidades y organismos del sector sanitario o asistencial, incluidos los prestadores públicos y privados del sector sanitario o asistencial, las entidades u organismos que llevan a cabo investigaciones en relación con estos sectores, y las instituciones, órganos y organismos de la Unión».

²⁰ Considerando 39 y art. 33.1 de la Propuesta de REEDS.

²¹ Art. 4(15) del RGPD: «datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud».

²² La solución empleada por legislador europeo para capturar normativamente esta paulatina ampliación del concepto de salud no ha consistido en ir añadiendo *ad hoc* nuevas categorías especiales de datos, sino en ir expandiendo el alcance de aquellas ya existentes (v.g. datos relativos a la salud y datos genéticos). En este sentido, vid. también: DE MONTALVO JAASKELÄINEN, «Ethical and legal requirements for biomedical research involving health data in the context of the COVID-19 pandemic: is informed consent still playing the leading role?», *BioLaw Journal*, Special Issue 2, 2021, pp. 157 ss.; y COTINO HUESO, «El alcance e interacción del régimen jurídico de los

Notoriamente, la definición del RGPD comprende no solo los datos personales directamente relacionados con la salud («datos relativos a la salud física o mental de una persona física»), sino también aquellos que indirectamente pudieran revelar aspectos relacionados con la misma («datos que revelen información sobre su estado de salud física o mental pasado, presente o futuro»). Pues bien, por si fuera poco, la noción de «datos de salud electrónicos personales» adiciona a lo anterior la de «datos genéticos» en el sentido del RGPD, otra categoría también amplísima²³ que deberá matizarse y limitarse de suerte que comprenda únicamente, en el contexto del EEDS, aquellos datos genéticos de carácter personal que se encuentren relacionados con o que sean relevantes para la salud humana, algo que la Propuesta no lleva a cabo de manera expresa²⁴.

Por último y como resultado de lo anterior, resulta pertinente llevar a cabo una precisión terminológica a los efectos de evitar futuras confusiones y problemas aplicativos con el texto del REEDS: la traducción del término «*electronic health data*» que aparece en el texto original de la Propuesta se ha llevado a cabo, de una manera jurídicamente desafortunada e imprecisa, como «dato sanitario electrónico». Tal deficiencia se encuentra presente a lo largo de toda la Propuesta, inclusive en su propia designación («Espacio Europeo de Datos Sanitarios») hasta el punto en que está siendo repetida literalmente y, a nuestro juicio, de forma equívoca por doctrina y autoridades públicas. Ello no es sino una inoportuna confusión entre los términos «*health data*» y «*healthcare data*» que equivaldrían a lo que conocemos, respectivamente, como «datos de salud» y «datos sanitarios», siendo así que este último denota un ámbito considerablemente más estricto: datos obtenidos y utilizados en y por las instituciones sanitarias, en el contexto de las relaciones de prestación de asistencia médica o sanitaria²⁵. Evidentemente, esta no es, en absoluto, la voluntad del legislador europeo, cuyo objetivo parece ser justo el contrario²⁶: consolidar un Espacio para la circulación y reutilización de datos de salud electrónicos en sentido amplio, no solo de aquellos coligados a los tradicionales contextos médicos y sanitarios. Así pues, debería descartarse el uso de la expresión «dato sanitario electrónico» a efectos de la Propuesta y sustituirla por la más adecuada de «dato de salud electrónico», en la medida en que la primera se encuentra hoy día en desuso y no permite capturar normativamente todos los aspectos y circunstancias relacionadas directa o indirectamente con una aproximación holística a la salud; incluyendo las nuevas fuentes de datos y su posible generación, recogida o tratamiento en una multiplicidad de entornos más allá de contextos clínicos, médicos o sanitarios.

datos personales y big data relacionado con la salud y la investigación biomédica», *Revista de Derecho y Genoma Humano: Genética, Biotecnología y Medicina Avanzada*, 52, 2020, pp. 57 ss.

²³ Art. 4(13) del RGPD: «datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona» (el subrayado es nuestro). Cabe señalar que se trata de una definición enunciada, asimismo, en términos amplios puesto que comprende, por un lado, tanto las características genéticas hereditarias o germinales como somáticas o adquiridas y, por otro, tanto las que aporten información sobre la salud como sobre la fisiología de la persona. Por ende, la concepción se realiza en términos que no se refieren exclusivamente a informaciones relativas a la salud de la persona.

²⁴ Sí que lo haría, en cambio, de manera implícita cuando alude en su listado del art. 33.1 a «datos genómicos pertinentes sobre patógenos que repercuten en la salud humana» o «datos genéticos, genómicos y proteómicos humanos» (el subrayado es nuestro).

²⁵ ABERASTURI GORRIÑO, *La protección de datos en la sanidad*, 2013. También en este sentido vid.: MURILLO DE LA CUEVA, «La publicidad de los archivos judiciales y la confidencialidad de los datos sanitarios», *VII Congreso Nacional de Derecho Sanitario*, 2000.

²⁶ También en este sentido puede verse: QUINN, «Is the GDPR and Its Right to Data Portability a Major Enabler of Citizen Science?», *Global Jurist*, 18(2), 2018.

2.2. Uso secundario versus tratamiento ulterior de datos personales

El uso secundario de datos de salud electrónicos constituye, como se ha anticipado, uno de los tres ejes vertebradores de la flamante Propuesta de REEDS. Por «uso primario» de datos de salud electrónicos se entiende el tratamiento de tales datos «para la prestación de servicios sanitarios con el fin de evaluar, conservar o restablecer el estado de salud de la persona física a la que se refieren dichos datos»²⁷. Por tanto, generalmente, el uso primario es aquél que se lleva a cabo en el contexto de la prestación de la asistencia sanitaria, incluyendo la prescripción, dispensación y provisión de medicamentos y de productos sanitarios, así como los servicios pertinentes de seguridad social, administrativos o de reembolso. Por su parte, se define «uso secundario» de datos de salud electrónicos como todo tratamiento de datos para los fines establecidos por el art. 34.1 de la Propuesta, precepto que introduce, como se verá, el listado de fines y usos permitidos ex lege. Ello permite incluir aquellos datos de salud electrónicos «recogidos inicialmente en el contexto de un uso primario», pero también aquellos «recogidos para un uso secundario»²⁸.

Esto último, si bien pudiera parecer una suerte de trabalenguas jurídico, es en realidad un elemento clave para comprender el sentido de la expresión y diferenciarla de otras anejas como la de «tratamiento ulterior de datos personales» empleada por el RGPD. En pocas palabras, lo que viene a sugerir es que, aunque en el contexto del Espacio los datos de salud electrónicos se recojan primordialmente en ámbitos sanitarios o asistenciales, ello no excluye de la obligación de puesta a disposición para usos secundarios a aquellos datos que pudieran proceder originalmente de otras fuentes (v.g. asociaciones profesionales, instituciones públicas, personas investigadoras, aseguradoras, etc.) o que se hubieran recogido con otros fines²⁹. De este modo, encontraremos tratamientos iniciales de datos según el RGPD que no encajarán en el concepto de «uso primario» vislumbrado por la Propuesta sino, más bien, en el de «uso secundario», pero respecto de los cuales aplicaría igualmente la obligación legal de puesta a disposición³⁰. Esta compleja interacción probablemente se comprenda mejor con un ejemplo. Piénsese en un proyecto de investigación o en un ensayo clínico que lleva a cabo una recogida prospectiva de los datos. O en un biobanco o un repositorio de datos que se crea y obtiene los datos, precisamente, con el fin primigenio de hacerlos disponibles para otros estudios. En ambos escenarios la finalidad de la recogida inicial no es otra que la investigación científica entendida en sentido amplio, pese a lo cual, bajo el régimen del REEDS, seguirán catalogándose como usos secundarios.

Esta categorización que se realiza de los usos secundarios es ambigua y tiende a desdibujar todavía más la ya dificultosa distinción conceptual con la figura del tratamiento ulterior de datos personales del RGPD³¹. Ambas expresiones suelen ser invocadas indistintamente con gran asiduidad, aunque no resulten del todo equiparables. De hecho, el concepto de «usos secundarios» es impropio de la jerga de la protección de datos personales ya que alude, de un

²⁷ Art. 2.2 letra d) de la Propuesta de REEDS.

²⁸ Art. 2.2 letra e) de la Propuesta de REEDS.

²⁹ Esto es, precisamente, lo que pretende dar a entender el Considerando 38 de la Propuesta.

³⁰ En este mismo sentido y entre otras: KISELEVA/DE HERT, «Creating a European Health Data Space: obstacles in four key legal areas», *European Pharmaceutical Law Review*, 5(1), 2021, p. 23; SLOKENBERGA, «Scientific research regime 2.0? Transformations of the research regime and the protection of the data subject that the proposed EHDS regulation promises to bring along», *Technology and Regulation*, 2022, p. 141.

³¹ Crítica compartida por CEPD y SEPD, Dictamen Conjunto 03/2022 sobre la Propuesta de REEDS (cit.), p. 13.

modo un tanto genérico, a todos aquellos usos que sean significativamente distintos respecto del contexto, origen o finalidades primigenias de los datos. Generalmente, la distinción entre usos primarios y secundarios se lleva a cabo con atención al ciclo de vida completo de los datos, desde su origen hasta su eventual supresión o desaparición definitiva³². Empero, en el caso del EEDS, como se ha visto, no siempre se cumplirá con lo anteriormente dispuesto, en la medida en que la calificación de un uso como primario o secundario se hará, en última instancia, por la vía de su encaje en las categorías preestablecidas por la norma.

Por su parte, ni para la protección de datos en general ni para el RGPD en particular opera dicho concepto de «usos secundarios», siendo la construcción legal más próxima aquella ya aludida de «tratamiento ulterior de datos personales». A saber, toda actividad de tratamiento que el responsable lleva a cabo con posterioridad a la recogida inicial (directa o indirecta) de los datos personales³³. A tales efectos, no cabe hablar de «usos primarios» sino de «actividad de tratamiento inicial», que será siempre la recogida de los datos personales por un responsable del tratamiento; ni de «usos secundarios» sino, más bien, del conjunto de actividades subsiguientes a la recogida (v.g. almacenamiento, organización, conservación, análisis, etc.), que serán tratamientos ulteriores. Así pues, el foco no se sitúa en el ciclo de vida completo de los datos sino en la fase concreta del tratamiento, es decir, en el conjunto de actividades de tratamiento llevadas a cabo por un responsable desde el momento en que obtiene directa (de la persona interesada) o indirectamente (de otro responsable) los datos personales³⁴. El origen, contexto o uso primigenio de los datos, previos a la obtención por ese responsable, resultan indiferentes para su eventual consideración como un tratamiento ulterior³⁵. Lo relevante para la protección de datos es que la recogida inicial se lleve a cabo con una finalidad específica y que cualquier tratamiento ulterior resulte compatible con los fines de la recogida inicial, sin que la proveniencia primigenia de los datos pueda condicionar en modo alguno su categorización legal como tratamiento ulterior.

Como puede comprobarse, la interrelación entre ambas figuras es compleja y no ha sido convenientemente abordada por la Propuesta REEDS. Por ello, todo parece indicar que tan ardua tarea deberá ser acometida posteriormente por parte de las autoridades de control nacionales y/o europeas; lo que probablemente dificultará la congruencia teórica y práctica entre ambas figuras y cuerpos normativos, siquiera en sus estadios iniciales de coexistencia.

³² AEPD, «Aproximación a los Espacios de Datos desde la perspectiva del RGPD», cit., p. 13. Por ejemplo, la recogida de datos en el curso de la asistencia sanitaria evoca típicamente un uso primario. Toda reutilización de esos datos en otros contextos o para otros fines que sean diferentes de la propia asistencia sanitaria (v.g. investigación científica, elaboración de estadísticas, mejora del funcionamiento del sistema sanitario, etc.) será considerado un uso secundario, en la medida en que difiere significativamente del contexto o finalidad originarias de los datos si atendemos a su ciclo de vida completo.

³³ Art. 5.1, letra b) y Considerando 50 del RGPD.

³⁴ BECKER, et. al. «Secondary Use of Personal Health Data: when is it “further processing” under the GDPR and what are the implications for data controllers?», *European Journal of Health Law*, 30(2), 2022, p. 146.

³⁵ Cabe matizar que, si bien el origen y contexto primigenios son indiferentes a los meros efectos de considerar efectivamente esa actividad como un tratamiento ulterior de datos personales, tales factores sí resultarán relevantes, en cambio, a la hora de evaluar la compatibilidad de los fines de la recogida inicial con los del tratamiento ulterior correspondiente ex art. 6.4 del RGPD.

3. Usos secundarios permitidos y usos secundarios prohibidos

3.1. Usos secundarios permitidos (art. 34): especial alusión a la investigación científica y la Inteligencia Artificial

Como se anticipaba supra, el art. 34.1 de la Propuesta de REEDS introduce un listado exhaustivo y cerrado de fines del tratamiento expresamente permitidos o, dicho de otro modo, de usos secundarios respecto de los cuales aplicará la obligación legal de puesta a disposición de los datos por parte de sus titulares. Son un total de ocho que, sin embargo, pueden clasificarse en dos grupos bien diferenciados por razón de la naturaleza de los titulares de datos que pueden presentar las correspondientes solicitudes de acceso a datos:

i) Usos secundarios permitidos exclusivamente para organismos del sector público e instituciones y organismos de la UE en el ejercicio de sus funciones públicas. Incluirá también aquellos terceros a quienes se encomiende el ejercicio de dichas funciones públicas³⁶. Se trata de los fines mencionados en las letras a), b) y c) del art. 34.1 de la Propuesta y que se refieren a aquellos tradicionalmente coligados a cláusulas de «interés público», a saber:

- Las actividades de interés público en el ámbito de la salud pública y la salud laboral, como la protección contra las amenazas transfronterizas graves para la salud, la vigilancia de la salud pública o la garantía de unos niveles elevados de calidad y seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios.
- El apoyo a los organismos del sector público, incluidas las autoridades reguladoras, en el sector sanitario o asistencial, en el desempeño de sus funciones.
- La elaboración de estadísticas oficiales nacionales, plurinacionales y de la Unión relativas al sector sanitario o asistencial.

ii) Usos secundarios permitidos para cualquier persona física o jurídica. Lo que incluye, además de los organismos e instituciones públicas mencionadas en el punto anterior, cualquier persona o entidad público-privada o privada, con o sin ánimo de lucro. Estos usos secundarios comprenden, en particular, los siguientes:

- Las actividades de educación o de enseñanza en el sector sanitario o asistencial.
- La prestación de asistencia sanitaria personalizada (medicina personalizada).
- La investigación científica relacionada con el sector sanitario o asistencial.
- Las actividades de desarrollo e innovación de productos o servicios que contribuyan a la salud pública o a la seguridad social, o que garanticen niveles elevados de calidad y seguridad de la asistencia sanitaria, de los medicamentos o productos sanitarios.

³⁶ Art. 33.2 de la Propuesta de REEDS.

- El entrenamiento, la prueba y la evaluación de algoritmos, también con respecto a los productos sanitarios, los sistemas de IA y las aplicaciones sanitarias digitales, que contribuyan a la salud pública o a la seguridad social.

Debe llamarse la atención sobre estos tres últimos usos secundarios habilitados por la Propuesta «para cualquier persona física o jurídica». Compartimos, en este sentido, la preocupación manifestada por el CEPD y el SEPD³⁷ y por una parte de la doctrina³⁸ y destacamos la necesidad de llevar a cabo una enmienda a este respecto.

Primeramente y, salvo que se remedie en su versión final, todo parece indicar que el REEDS será otra oportunidad legislativa perdida para delimitar con claridad el concepto y los contornos de la «investigación científica» en relación con los tratamientos de datos de carácter personal y, en definitiva, para otorgar una mayor seguridad jurídica a las personas u organizaciones que persigan legítimamente tales finalidades. La Propuesta parece limitarse a seguir la amplia pero ambigua concepción del RGPD³⁹ matizando únicamente que la investigación deberá hallarse relacionada «con el sector sanitario o asistencial». Con ello, renuncia a fijar unas condiciones mínimas exigibles a la cualificación de una finalidad como propiamente de «investigación científica» tales como la aplicación de normas, estándares o garantías éticas y metodológicas. En última instancia, tampoco se esclarece si los fines de investigación científica que legitimarían un acceso a datos en el seno del EEDS incluirían únicamente aquellos susceptibles de producir un beneficio o bienestar para un grupo de personas o para el interés general de la sociedad en su conjunto. La respuesta a esto último, entendemos, debe ser afirmativa, puesto que de otro modo ello no respetaría el objetivo de la Propuesta de priorizar el acceso a los datos para usos secundarios que contribuyan al interés general de la sociedad⁴⁰. Por fin y por lo que atañe particularmente al caso español, consideramos prioritario resolver la potencial interacción entre la referida noción de «investigación científica relacionada con el sector sanitario o asistencial» y aquellas otras contenidas en la Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales (investigación en salud, biomédica y en salud pública)⁴¹ que, de no llevarse a cabo con rigurosidad y prontitud, podría erigirse en una nueva fuente de conflictos y asimetrías.

³⁷ CEPD y SEPD, Dictamen Conjunto 03/2022 sobre la Propuesta de REEDS, cit., p. 22.

³⁸ SHABANI, «Will the European Health Data Space change data sharing rules?», *Science*, 375, 2022, pp. 1357 ss.; MARELLI, et. al, «The European Health Data Space: too big to succeed?», *Health Policy*, 135, 104861, 2023.

³⁹ Considerando 44 de la Propuesta de REEDS: «El suministro de datos también debe apoyar actividades relacionadas con la investigación científica (incluida la investigación privada), el desarrollo y la innovación». Ello replica en gran medida lo dispuesto por el Considerando 159 del RGPD: «El tratamiento de datos personales con fines de investigación científica debe interpretarse, a efectos del presente Reglamento, de manera amplia, que incluya, por ejemplo, el desarrollo tecnológico y la demostración, la investigación fundamental, la investigación aplicada y la investigación financiada por el sector privado».

⁴⁰ Considerando 41 de la Propuesta de REEDS: «El acceso a los datos para uso secundario debe contribuir al interés general de la sociedad». De la misma opinión es MARTÍNEZ MARTÍNEZ, para quien el EEDS representa «una concepción que integra los intereses colectivos haciéndolos compatibles con todos aquellos intereses individuales y particularmente con la garantía de los derechos fundamentales, la libertad de creación científica y técnica o la libertad de empresa». En relación con esto último, vid: MARTÍNEZ MARTÍNEZ, «Digitalización y construcción normativa de los Espacios Europeos de Datos: retos para el sector público», *La Ley Privacidad*, 13, 2022, p. 9.

⁴¹ Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. «BOE» núm. 294, de 06/12/2018. Vid. en particular su Disposición Adicional Decimoséptima, apartado segundo.

En segundo y último lugar, consideramos particularmente problemáticos los usos secundarios habilitados para «actividades de desarrollo e innovación de productos o servicios» y para «el entrenamiento, la prueba y la evaluación de algoritmos»; o, más bien, la forma en que quedan reflejados y descritos por el REEDS. De acogerse, como parece, la concepción amplia de fines investigación científica proclamada por el RGPD, ambos usos deberían quedar necesariamente subsumidos por esta puesto que abarca, en sentido lato, el desarrollo tecnológico, la demostración, la investigación aplicada y la investigación financiada por el sector privado. En lo que se refiere, en particular, a los usos secundarios para el desarrollo de algoritmos y sistemas de IA, su inclusión expresa y diferenciada constituye a nuestro juicio una clara alteración del principio normativo de neutralidad tecnológica, de suerte que, con ello, el legislador estaría confiriendo primacía al desarrollo o demostración de una o varias herramientas o tecnologías en detrimento de otras coetáneas o venideras. Finalmente, si bien es cierto que la Inteligencia Artificial parece anticipar una miríada de aplicaciones y usos beneficiosos para la prestación de la asistencia sanitaria o la investigación, no existe a día de hoy un grado de evidencia científica suficiente que justifique la concesión de esta suerte de régimen *sui generis*⁴².

Por todo lo anterior, la Propuesta debería evitar aludir por separado a los usos secundarios para el desarrollo de algoritmos o sistemas de Inteligencia Artificial o, en caso de que se considerase indispensable mantenerlo por razones de política legislativa, debería realizarse a efectos meramente ilustrativos de lo que se entiende por un uso secundario de investigación científica en sentido amplio. Con ello, por un lado, se preserva la neutralidad de la norma para con la tecnología a desarrollar o demostrar (así como la libertad de elección del método científico) y, por otro, se evita la posible inobservancia por parte de ciertos actores tradicionalmente ajenos al sector investigativo de las garantías, principios o procedimientos aplicables a tales actividades. Lo que se instituye, en definitiva, crucial a fin de evitar la proliferación de prácticas o usos abusivos disfrazadas de fines de investigación científica genuina. Este ha sido, de hecho, el sentido de la enmienda formulada por el Comité LIBE del Parlamento Europeo⁴³.

3.2. Usos secundarios prohibidos (art. 35)

Para concluir con este punto, además del ya indicado listado de usos permitidos, el REEDS se refiere a una serie de usos secundarios que se encuentran, en todo caso, prohibidos⁴⁴. Cabe cuestionarse el sentido de esta disposición, en la medida en que podría entenderse que cualquier uso no permitido explícitamente por el art. 34.1 anteriormente referido habría de quedar,

⁴² TERZIS, «Compromises and Asymmetries in the European Health Data Space», *European Journal of Health Law*, 30(3), 2022, p. 363.

⁴³ European Parliament (Committee on the Environment, Public Health and Food Safety & Committee on Civil Liberties, Justice and Home Affairs), *Draft Report on the proposal for a Regulation on the European Health Data Space*, 2022/0140(COD) 10/02/2023. Propuesta de enmienda núm. 89, p. 57.

⁴⁴ Se encuentran prohibidos, en virtud de lo dispuesto por el art. 35 de la Propuesta de REEDS aquellos usos secundarios cuyo fin sea: a) tomar decisiones perjudiciales para una persona física sobre la base de sus datos sanitarios electrónicos; b) tomar decisiones en relación con una persona física o grupos de personas físicas para excluirlas del beneficio de un contrato de seguro o modificar sus cotizaciones y primas de seguro; c) llevar a cabo actividades de publicidad o comercialización dirigidas a profesionales sanitarios, organizaciones del sector o personas físicas; d) facilitar el acceso a los datos sanitarios electrónicos a terceros no mencionados en el permiso de datos, o ponerlos a su disposición de algún otro modo; y e) desarrollar productos o servicios que puedan perjudicar a las personas y a las sociedades en general, incluidas, entre otras, las drogas ilícitas, las bebidas alcohólicas, los productos del tabaco o los bienes o servicios diseñados o modificados de manera que contravengan el orden público o la moral.

automáticamente, proscrito o excluido de ser alegado en una solicitud de acceso a datos. A grandes rasgos, el componente común de todos los usos prohibidos designados radica en su potencial perjuicio para las personas físicas o para el interés general, de manera que actúa como cláusula de cierre para garantizar la buena fe de los usuarios de los datos y el respeto de la moral y el orden público. Con ello, viene a proclamar una salvaguarda reforzada frente a determinadas prácticas discriminatorias o abusivas⁴⁵ o ciertas conductas o finalidades de tratamiento que hayan sido social o moralmente reprobadas por la ciudadanía⁴⁶.

Nos parece oportuno finalizar con una breve reflexión de ética jurídica: ¿quién y con arreglo a qué criterios podrá decidir cuáles son los usos permitidos y prohibidos? No deja de ser una pregunta retórica pues trata de una decisión, en última instancia, política; lo que no ha de significar que el legislador *motu proprio* sea el mejor situado para adoptarla⁴⁷. A nuestro juicio, la única forma de que el REEDS responda efectivamente a los bienintencionados objetivos para los que ha sido concebido sin menoscabar la confianza de la sociedad en el sistema propuesto, es la articulación de un proceso transparente y participativo que dé voz a las diferentes partes interesadas a la hora de mantener los usos secundarios existentes o de introducir cualesquiera otros inicialmente no previstos. La aceptación social de los usos secundarios permitidos o la confianza pública en los mecanismos de gobernanza propuestos no vendrán automáticamente otorgadas por la legitimidad jurídica de la norma⁴⁸. De otro modo, el Espacio podría correr el riesgo de seguir la estela de las (no pocas) iniciativas que se han llevado a cabo en un sentido similar y que han terminado decayendo por una prematura quiebra de la confianza de las partes afectadas y de la sociedad en su conjunto.

⁴⁵ Con lo que la Propuesta vendría a alinearse con la prohibición proclamada, entre otros, por el art. 14 de la Declaración Internacional de la UNESCO sobre Datos Genéticos Humanos, o por el Considerando 54 del RGPD («este tratamiento de datos relativos a la salud por razones de interés público no debe dar lugar a que terceros, como empresarios, compañías de seguros o entidades bancarias, traten los datos personales con otros fines»).

⁴⁶ Valga como ilustración un estudio recientemente llevado a cabo sobre las actitudes de la ciudadanía europea respecto a la reutilización de sus datos de salud, que evidenció una aversión generalizada frente a: i) la comercialización con fines de lucro de tales datos por parte de compañías privadas; ii) el uso en contextos laborales o por parte de los empleadores; iii) el uso por parte de compañías aseguradoras para denegar contratos de seguro o subir primas; y iv) su uso con fines publicitarios y de marketing. Vid. SKOVGAARD, et.al, «A review of attitudes towards the reuse of health data among people in the European Union: the primacy of purpose and the common good», *Health Policy*, 123(6), 2019. En un sentido similar cabría invocar, asimismo, los trabajos preliminares a la Propuesta de REEDS llevados a cabo en el seno de la iniciativa TEHDAS, que evidenciaron una opinión mayoritariamente contraria a la reutilización de datos de salud electrónicos por parte de compañías de seguros, empleadores, entidades bancarias o multinacionales. Towards the European Health Data Space Joint Action (TEHDAS), *Healthy Data – an online citizen consultation about health data reuse*, 2022.

⁴⁷ Vid. también, en sentido similar: KAPLAN, «How Should Health Data Be Used? Privacy, Secondary Use, and Big Data Sales», *Cambridge Quarterly of Healthcare Ethics*, 25(2), 2016, pp. 312 ss; y FORGÓ, «My health data – your research: some preliminary thoughts on different values in the General Data Protection Regulation», *International Data Privacy Law*, 5(1), 2015, p. 62.

⁴⁸ STAUNTON, Ciara, et al. «Ethical and social reflections on the proposed European Health Data Space», *European Journal of Human Genetics*, 2024, p. 4. Esto es de suma importancia si se tiene en cuenta que, con arreglo al REEDS, los datos podrán utilizarse para fines inicialmente no consentidos por las personas interesadas o que no hubieran podido prever en el momento en que se recogieron sus datos. Piénsese en los datos contenidos en las historias clínicas electrónicas y en lo inesperado que para los pacientes pudiera resultar que aquellos fueran eventualmente utilizados para desarrollar o entrenar algoritmos y sistemas de IA.

4. Componentes y actores principales del Espacio Europeo de Datos de Salud

El Espacio incorporará, previsiblemente, todo un conglomerado de nuevos actores y componentes que puede llegar a parecer un tanto abrumador a simple vista. Máxime, toda vez que aquéllos habrán de coexistir e interrelacionarse con los ya establecidos por la normativa de protección de datos, incluyendo sus principios básicos, roles (v.g. responsables y encargados del tratamiento, entre otros) o bases de licitud. A tal efecto, el REEDS se situaría en una posición de complementariedad con el RGPD en la que, aun sin desplazar sus disposiciones y principios generalmente aplicables, sí que los matiza o desarrolla en ciertos aspectos⁴⁹. En gran medida, porque el Espacio no es sino una pronta reacción legislativa frente a las carencias observadas durante el breve lapso de vigencia del RGPD y que afectan sobremanera al tratamiento de datos genéticos y datos relativos a la salud, en especial, en lo que a fines estadísticos, de archivo en interés público e investigación científica e histórica se refiere⁵⁰.

Así, en lo que concierne al uso secundario de datos de salud electrónicos, el EEDS prevé articular un sistema que opere sobre la base de cuatro actores o componentes principales: i) los titulares de datos; ii) los usuarios de datos; iii) los organismos de acceso a datos; y iv) una infraestructura para el acceso transfronterizo a datos (*HealthData@EU*).

4.1. Titulares de datos

Son todas aquellas personas físicas o jurídicas que constituyan entidades u organismos del sector sanitario o asistencial o que lleven a cabo investigaciones en relación con estos sectores, así como instituciones, órganos y organismos de la UE, que tienen la obligación de poner a disposición de los usuarios determinados datos de salud electrónicos. Núcleo que incluiría a prestadores de asistencia sanitaria, asociaciones u otras entidades sin ánimo de lucro o privadas que desempeñen un papel fundamental en el sector sanitario y otras que reciban financiación pública de la Unión o de los Estados miembros con fines de investigación, estadísticos u otros fines similares⁵¹. Quedan excluidas, no obstante, tanto de su consideración como titulares de datos, como de la obligación de puesta disposición de datos, las microempresas⁵². En líneas generales, comprende mayormente entidades, organizaciones u organismos del sector sanitario, asistencial o investigativo públicos y/o aquellas sin ánimo de lucro o privadas que se encuentren estrechamente vinculadas con las primeras o que reciban financiación pública para el desarrollo

⁴⁹ Tal y como dispone el Considerando 37 de la Propuesta, el Reglamento proporciona bases jurídicas de conformidad con el art. 6.1 del RGPD y excepciones al tratamiento de categorías especiales de datos de acuerdo con el art. 9.2 del RGPD para el uso secundario de datos de salud electrónicos personales. Asimismo, el texto provee de garantías adecuadas en el sentido del art. 89.1 del RGPD, tanto organizativas y de gobernanza (v.g. organismos de acceso a datos) como técnicas (v.g. seudonimización, entornos de tratamiento seguros).

⁵⁰ Como advertíamos en otra parte, la persistencia de ciertas cláusulas abiertas y de remisión a los Estados miembros (v.g. arts. 9.2.j, 9.4 o 89 del RGPD) han derivado en un escenario fragmentado incluso a nivel comunitario, dificultando notoriamente la labor interpretativa y aplicativa de los operadores jurídicos de determinados sectores. Vid.: RECUERO, «La investigación científica con datos personales genéticos y datos relativos a la salud: perspectiva europea ante el desafío globalizado», *Premios de Investigación en Protección de Datos Personales Emilio Aced*, Agencia Española de Protección de Datos, Madrid, 2019.

⁵¹ Art. 2.2.y) y Considerando 40 de la Propuesta de REEDS.

⁵² Considerando 40 y art. 33.2 de la Propuesta de REEDS.

de sus actividades. Así pues, se trata de una definición lo suficientemente comprensiva para abarcar, entre otros, centros sanitarios, hospitales, centros de investigación, biobancos, repositorios, registros poblacionales, instituciones académicas e, incluso, empresas farmacéuticas, prestadores de servicios y fabricantes de productos sanitarios.

El elemento que aglutina toda esta amalgama de actores bajo una designación común es la imposición de una obligación por el art. 33.1 de la norma: la puesta a disposición de una serie de categorías mínimas de datos de salud electrónicos para su uso secundario por parte de los usuarios de datos que así lo soliciten. Este precepto proclama e instituye una auténtica «obligación legal» en el sentido del art. 6.1, letra b) del RGPD que conmina a los titulares de los datos, en tanto responsables del tratamiento, a ponerlos a disposición de los usuarios de datos para los usos secundarios permitidos anteriormente descritos⁵³. Dicho de otro modo, tales actividades de puesta a disposición de datos personales, en la medida en que equivalen a un tratamiento ulterior, serán declaradas ex lege compatibles con la finalidad de la recogida inicial de los datos. Paralelamente, puesto que nos hallamos ante categorías especiales de datos personales (datos genéticos o datos relativos a la salud en el sentido del RGPD), el REEDS también proveería, por medio del meritado art. 33.1, de una o varias excepciones a la prohibición del tratamiento instituida por el art. 9.2 del RGPD. En este punto, la elección de la circunstancia concreta para levantar el veto del art. 9.1 no está del todo clara, pues dependerá del uso secundario al que pretendan destinarse los datos por parte del usuario, pero habrá de entenderse comprendida en todo caso en alguna de las letras h), i) o j) del art. 9.2 del RGPD.

4.2. Usuarios de datos

Son todas aquellas personas físicas o jurídicas que tienen acceso legítimo a los datos de salud electrónicos personales y que están autorizadas a utilizarlos con alguno de los fines del art. 34.1 REEDS, incluyendo usos no comerciales y comerciales⁵⁴. Como cabe apreciar, se trata de un conjunto ostensiblemente más comprensivo de personas y entidades que el de los titulares de datos y que integraría, básicamente, a «cualquier persona física o jurídica»⁵⁵. Por lo tanto, cualquier persona o entidad (pública o privada, con o sin ánimo de lucro) podrá legítimamente solicitar el acceso a los datos, con independencia del sector en que desarrolle su actividad. Contrasta ello con el círculo más restringido de los titulares de datos, que deben tratarse necesariamente de personas, entidades u organismos del sector sanitario, asistencial o investigativo. Como advierte TERZIS, tal sesgo en el núcleo de sujetos obligados puede terminar otorgando una notoria ventaja competitiva a grandes empresas tecnológicas que, aunque posean sendas filiales relacionadas con la salud digital o la investigación, quedarían expelidas de la obligación legal de facilitar el acceso a sus datos, pero sí podrían, en cambio, solicitar el acceso a aquellos conjuntos de datos del resto de entidades del sector sanitario, asistencial o

⁵³ Puede verse en este sentido el Considerando 37 de la Propuesta de REEDS.

⁵⁴ Art. 2.2, letra z) y Considerando 41 de la Propuesta de REEDS.

⁵⁵ Art. 45.1 de la Propuesta de REEDS: «Cualquier persona física o jurídica podrá presentar una solicitud de acceso a los datos para los fines mencionados en el artículo 34».

investigativo⁵⁶. De acogerse, las asimetrías informacionales entre las entidades del sector público y privado no harían sino exacerbarse⁵⁷.

Desde la perspectiva de la protección de datos personales, el usuario de datos deberá fundamentar jurídicamente su solicitud de acceso con arreglo a las letras e) o f) del art. 6.1 del RGPD ya que no podrá invocar, como decíamos, la obligación legal contenida en el art. 33.1 de la Propuesta, que resultará únicamente aplicable a los titulares. Así pues, para legitimar su acceso, el usuario únicamente podrá alegar el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos (que se encuentre reconocida por otra norma nacional o de la UE) o el interés legítimo, en cuyo caso las garantías aplicables serán las previstas por el REEDS. Finalmente, en lo que atañe a las excepciones para el tratamiento de categorías especiales de datos, nuevamente, el usuario deberá escoger entre aquellas del art. 9.2 del RGPD que sean más adecuadas a la finalidad pretendida y, concretamente, alguna de las letras h), i) o j). Con todo, la nueva norma no pretende, en absoluto, llevar a cabo una armonización de las bases de licitud ni de las circunstancias del art. 9.2 del RGPD en lo atinente a los usuarios de datos. Presumiblemente, la falta de determinación legislativa en este punto desembocará en la práctica en una limitación del acceso y disponibilidad efectivas de los datos en el contexto del EEDS, actuando la necesidad de justificar el interés público o legítimo subyacente a modo de criba de aquellas solicitudes de acceso potencialmente infundadas o desproporcionadas.

4.3. Organismos de acceso a datos

Son los organismos responsables de conceder el acceso a los datos de salud electrónicos para los usos secundarios permitidos. Su creación compete a los Estados miembros, que podrán crear uno o varios (v.g. uno estatal y/o para cada Comunidad Autónoma con competencias en la materia), pero que deberán designar uno como coordinador y punto de contacto nacional⁵⁸. La Propuesta no aclara si debe tratarse de organismos públicos y/o administrativos, limitándose a reconocer su variabilidad en términos de organización y tamaño, aunque todo parece indicar que sí deberán gozar de dicha consideración, en la medida en que se exige su independencia funcional y la asignación de recursos financieros, físicos y humanos propios. Algunos autores arguyen que esto supone la atribución de un elevado grado de autonomía a los Estados miembros, propiciando entornos y enfoques divergentes y fragmentados e, incluso, el siempre latente riesgo de *forum-shopping*⁵⁹. En cambio, a nuestro parecer, el REEDS dedica no pocos preceptos a detallar y armonizar las funciones y obligaciones de estos organismos (arts. 36 a 39), las posibles tasas y sanciones (arts. 42 y 43), o el contenido y las condiciones mínimas de las solicitudes de acceso y el permiso de datos (arts. 45 y 46, respectivamente). Adicionalmente, no debe pasarse por alto que el EEDS se instituye, ante todo, como una infraestructura eminentemente federada que

⁵⁶ TERZIS, *European Journal of Health Law*, 30(3), 2022, p. 363.

⁵⁷ Así lo advierte el PARLAMENTO EUROPEO a través de su Comisión de Industria, Investigación y Energía (ITRE). Vid. en este sentido: ITRE, *Study on the European Health Data Space*, 2022, p. 49.

⁵⁸ Considerando 42 y art. 36 de la Propuesta de REEDS.

⁵⁹ HORGAN, et. al., «European Health Data Space – An opportunity now to grasp the future of data-driven healthcare», *Healthcare*, 10(9), 2022, p. 8.

respete la soberanía estatal e integre las plataformas y nodos preexistentes, en buena medida, por las propias exigencias derivadas de las limitaciones competenciales de la UE⁶⁰.

La mayor preocupación en este punto radica, desde nuestro punto de vista, en las interacciones de estos organismos con otros comités y órganos preexistentes y que desempeñan ya funciones o roles similares. Así, por ejemplo, no queda para nada clara su relación con los Comités de Acceso a Datos (DACs, por sus siglas en inglés) que durante décadas han venido instaurándose como «guardianes» del acceso a datos en repositorios, biobancos, consorcios de investigación y plataformas y con quienes podrían llegar a solaparse funcionalmente. Otro paradigma es el de los Comités de Ética correspondientes. La Propuesta de REEDS se limita a demandar «información sobre la evaluación de los aspectos éticos del tratamiento» con ocasión de las solicitudes de acceso a datos seudonimizados «cuando proceda y de conformidad con la legislación nacional» (art. 45.4, letra b) y a proclamar un deber genérico de cooperación con los comités de ética (art. 37.2, letra c). Previsión a todas luces insuficiente y que propiciará problemas de cohesión en los criterios de acceso a datos, especialmente en escenarios de solicitudes transfronterizas, habida cuenta de que la uniformización de los mecanismos legales o de gobernanza no resolverá por sí sola las divergencias jurisdiccionales o institucionales en las prácticas y procedimientos de evaluación de aspectos éticos del tratamiento. Por no hablar de que tales controles quedarían estrictamente circunscritos a determinadas solicitudes (v.g. aquellas realizadas con fines de investigación científica y, en particular, en salud o biomédica), descuidando la necesidad de examinar los aspectos éticos del tratamiento para el resto de los usos secundarios permitidos (v.g. ética en el desarrollo de sistemas de IA)⁶¹. Por ello, parece razonable que los organismos de acceso integren en su estructura un comité de ética o un grupo de personas expertas en la materia o, en su caso, designen uno o varios externos para llevar a cabo la evaluación de los aspectos éticos de las solicitudes⁶².

En lo que se refiere, por fin, a la interacción de lo dispuesto en este apartado con la normativa de protección de datos personales, el desempeño de las diversas funciones atribuidas a los organismos de acceso a datos ha de entenderse comprendida en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos, en el sentido del art. 6.1 letra e) y de las excepciones correspondientes del art. 9.2 incisos h), i) y j) del RGPD⁶³. En el momento en que se conceda el acceso a datos electrónicos personales a un usuario por parte del organismo, ambos serán considerados corresponsables del tratamiento, de conformidad y en las condiciones estipuladas en el permiso de datos correspondiente y hasta que concluya la actividad o

⁶⁰ Enfoque compartido por la AEDS: «El nuevo marco europeo no debe perder de vista que la organización y prestación de los servicios sanitarios es un ámbito de responsabilidad primaria de los Estados miembros, sin perjuicio del necesario respeto de la normativa europea de mínimos basada en otros títulos competenciales concurrentes y sin detrimento de un espacio común de datos europeo». ASOCIACIÓN ESPAÑOLA DE DERECHO SANITARIO, *Recomendaciones sobre el nuevo Espacio Europeo de Datos de Salud*, recomendación núm. 14.

⁶¹ STAUNTON, et al. *European Journal of Human Genetics*, 2024, pp. 3 ss.

⁶² MARTÍNEZ MARTÍNEZ, *La Ley Privacidad*, 13, 2022, p. 13. El autor propone una tercera vía consistente en la creación de un catálogo de comités (v.g. hospitalarios, universitarios) cuyas resoluciones pudieran convalidarse.

⁶³ Considerando 37 de la Propuesta de REEDS.

actividades de tratamiento en cuestión⁶⁴. Lo anterior confiere a los organismos de acceso un rol legal que va más allá del de meros intermediarios o «custodios» de los datos⁶⁵.

4.4. HealthData@EU

Es la infraestructura que conecta los puntos de contacto nacionales⁶⁶ y que faculta el acceso transfronterizo a datos de salud electrónicos para uso secundario a través de una plataforma central⁶⁷. La estructura del EEDS se disgrega en uno o más nodos federados que, aunque han de regirse bajo unas reglas y procedimientos comunes, operan con una cierta independencia funcional. Por consiguiente, cuando un usuario de datos solicita el acceso a conjuntos de datos ubicados en más de un Estado miembro o, en su caso, cuando el acceso se solicita por un usuario de datos sito en un Estado miembro diferente al lugar en el que se encuentran físicamente los datos, se precisa una suerte de plataforma que coordine a todos estos nodos y actores y provea de una pasarela y servicios comunes e integrados. Esta plataforma central se sustentará y será operada por la propia Comisión, quien prestará los servicios necesarios (incluyendo un entorno de tratamiento seguro) en tanto encargada del tratamiento⁶⁸. Por su parte, los nodos o puntos de contacto que intervengan en las correspondientes actividades o solicitudes actuarán como corresponsables del tratamiento⁶⁹.

Las posibilidades de esta infraestructura son realmente interesantes, puesto que no solo prevé integrar como nodos a los respectivos puntos de contacto nacionales. Adicionalmente, se podrán conectar a la plataforma instituciones, órganos y organismos de la UE que participen en la investigación o en la política sanitaria (v.g. la Agencia Europea de Medicamentos, el Consorcio de Infraestructuras de Investigación Europeas, el Foro Estratégico Europeo sobre Infraestructuras de Investigación) y hasta consorcios, repositorios, biobancos o bases de datos de investigación relacionadas con la salud⁷⁰. Finalmente, se contempla un mecanismo específico en virtud del cual podrán tener acceso a la infraestructura como participantes autorizados incluso organizaciones internacionales y nodos u organismos de acceso de terceros países.

Esto último presenta un enorme potencial para el impulso de los usos secundarios de datos a escala internacional y global, promoviendo un acceso remoto seguro a datos electrónicos de salud con diversos fines a través de entornos restringidos y controlados que eviten su transmisión física fuera de las fronteras de la Unión o del Espacio Económico Europeo. Inclusive, en el mejor

⁶⁴ Arts. 51 y 46.14, respectivamente, de la Propuesta de REEDS.

⁶⁵ MOLNÁR-GÁBOR, et al. «Bridging the European Data Sharing Divide in Genomic Science», *Journal of Medical Internet Research*, 24(10), 2022, p. 8.

⁶⁶ Art. 2.2, letra u) «punto de contacto nacional para el uso secundario de datos sanitarios electrónicos»: una pasarela organizativa y técnica que permite el uso secundario transfronterizo de datos sanitarios electrónicos, bajo la responsabilidad de los Estados miembros. Estos puntos de contacto podrán ser los representantes o coordinadores de los organismos nacionales de acceso a datos (art. 52.1 REEDS).

⁶⁷ Art. 2.2, letra v) «plataforma central para el uso secundario de datos sanitarios electrónicos»: una plataforma de interoperabilidad creada por la Comisión, que presta servicios para apoyar y facilitar el intercambio de información entre los puntos de contacto nacionales para el uso secundario de datos sanitarios electrónicos.

⁶⁸ Art. 52, apartados 9º y 10º de la Propuesta de REEDS.

⁶⁹ Art. 52.11 de la Propuesta de REEDS.

⁷⁰ Considerando 55 y art. 52, apartados 3º y 4º de la Propuesta de REEDS.

de los escenarios, ello podría constituir un muy necesario punto de inflexión a la hora de aplicar «en bloque» el régimen de transferencias internacionales de datos personales contenido en el Capítulo V del RGPD o, en su caso, abogar por una mayor adaptabilidad de sus disposiciones. Sea como fuere, se trata de una vía incipiente y poco explorada por la literatura⁷¹, de ahí que resulte conveniente postergarlo para su estudio más exhaustivo en el futuro.

5. Condiciones y procedimientos para el acceso a datos de salud electrónicos en el Espacio Europeo de Datos de Salud

El acceso a datos por parte de los usuarios en el seno del EEDS se llevará a cabo mediante la presentación de una solicitud de acceso a datos ante un organismo de acceso o, en determinados supuestos, directamente ante el titular correspondiente. El contenido mínimo de la solicitud deberá ajustarse a lo dispuesto por el futuro Reglamento⁷². Como regla general, la solicitud de acceso se realizará para datos que se encuentren anonimizados. El usuario podrá solicitar el acceso a datos seudonimizados si, adicionalmente: i) fundamenta su necesidad para alcanzar los fines pretendidos; ii) invoca una base jurídica y, en su caso, una excepción para el tratamiento de categorías especiales de datos en el sentido de los arts. 6.1 y 9.2 del RGPD, respectivamente; y iii) si fuera exigido por la legislación nacional aplicable, facilita la información correspondiente sobre la evaluación de los aspectos éticos del tratamiento de datos o proyecto de investigación. Asimismo, el acceso se producirá en todo caso a través de un entorno de tratamiento seguro que incluya las debidas medidas técnicas, organizativas y de seguridad y, en particular, aquellas mencionadas expresamente por el art. 50 de la Propuesta de REEDS.

Recibida la solicitud de acceso se procederá a tramitar el procedimiento correspondiente, que se trata de un proceso reglado y que es común a nivel europeo, a fin de garantizar la uniformidad de criterios entre Estados miembros. Esencialmente, la Propuesta prevé dos clases de procedimientos: uno *general*, aplicable a las solicitudes de acceso que impliquen varios conjuntos de datos de dos o más Estados miembros, y otro *simplificado*, para aquellos supuestos en que un usuario solicite el acceso a datos ante un titular y de un único Estado miembro. Naturalmente, aunque existen algunas diferencias en las que más adelante se ahondará, comparten la gran mayoría de componentes. Así, en ambos casos el procedimiento finaliza con la expedición de un «permiso de datos», una decisión administrativa por la que se concede el acceso a los datos a los usuarios solicitantes y para los usos especificados en su solicitud⁷³. Este permiso será el que establezca las condiciones generales aplicables al acceso y deberá incluir, entre otros: los tipos y el formato de los datos, la finalidad para la que se facilitan, la duración del permiso, las

⁷¹ Es más, el potencial de este cauce solo ha sido advertido, hasta la fecha, en otra publicación en que abordábamos esta misma cuestión de manera preliminar: MOLNÁR-GÁBOR, et al., *Journal of Medical Internet Research*, 24(10), 2022, pp. 8 ss.

⁷² Art. 45.2 de la Propuesta de REEDS. La solicitud de acceso a datos incluirá: a) una explicación detallada del uso previsto de los datos, especificando el fin o fines de los contemplados en el art. 34.1; b) una descripción de los datos de salud electrónicos solicitados, su formato y fuentes de datos, cuando sea posible, incluida la cobertura geográfica cuando se soliciten datos de varios Estados miembros; c) una indicación de si los datos deben facilitarse en un formato anonimizado; d) cuando proceda, una explicación de los motivos por los que se solicita el acceso a datos en un formato seudonimizado; e) una descripción de las garantías previstas para evitar otros usos no autorizados; f) una descripción de las garantías previstas para proteger los derechos e intereses de los titulares de datos y de las personas físicas afectadas; g) una estimación del período de tiempo necesario; y h) una descripción de las herramientas y recursos informáticos necesarios.

⁷³ Propuesta de REEDS, art. 2.2, letra a) «permiso de datos».

características técnicas y herramientas para su tratamiento en entornos seguros o, en su caso, las tasas a abonar por el usuario⁷⁴. La duración del permiso será aquella estrictamente necesaria para el cumplimiento de los fines para los cuales se solicita el acceso, sin que pueda exceder de cinco años⁷⁵. Excepcionalmente, el usuario podrá solicitar una única prórroga de hasta cinco años adicionales, siempre que lo justifique debidamente un mes antes de la expiración del primer plazo concedido.

Finalmente, la Propuesta también prevé otras obligaciones comúnmente aplicables con independencia del procedimiento seguido. Primera, impone a todo usuario el deber de informar al organismo de acceso o titular correspondiente de cualquier hallazgo imprevisto o conclusión clínicamente significativa para la salud de las personas físicas⁷⁶. Segunda, conmina a los usuarios a hacer públicos los resultados, servicios o productos resultantes dentro de los dieciocho meses siguientes a la finalización del plazo concedido para el permiso⁷⁷. Ello deberá incluir el debido reconocimiento de las fuentes de acceso y, si fuera el caso, el retorno de los conjuntos de datos enriquecidos al titular correspondiente, a fin de que pueda, nuevamente, hacerlos disponibles para su uso secundario por otros usuarios.

Seguidamente, como colofón, nos referimos por separado a las dos clases de procedimientos de acceso existentes junto con sus especificidades.

5.1. Procedimiento ordinario

Se trata de aquél generalmente aplicable cuando la solicitud de acceso requiera la combinación de varios conjuntos de datos, se refiera a dos o más titulares de datos o sea de carácter plurinacional, esto es, involucre a dos o más Estados miembros. En tales supuestos, la solicitud de acceso deberá presentarse siempre ante un organismo de acceso, el de elección del usuario, pues rige el «principio de solicitud única». Ello permite a los usuarios presentar la solicitud de acceso ante cualquier organismo, siendo este último el responsable de trasladar su recepción al resto de involucrados, lo que se llevará a cabo por medio de la ya mencionada plataforma *HealthData@EU*.

Recibida la solicitud, el organismo de acceso dispondrá de un plazo de dos meses, prorrogables por otros dos si así lo exigiese la complejidad de la petición⁷⁸, para conceder el permiso de datos o denegar de forma razonada la solicitud de acceso. Expedido el permiso, el organismo solicitará al titular o titulares el acceso a los datos correspondientes y los pondrá a disposición del usuario solicitante a través de un entorno de tratamiento seguro. Este último paso deberá llevarse a cabo por el organismo de acceso dentro de los dos meses siguientes contados a partir de la recepción de los conjuntos de datos del titular o titulares, que podrá igualmente prorrogarse por otros dos meses más en caso de peticiones complejas⁷⁹.

⁷⁴ Art. 46.6 de la Propuesta de REEDS.

⁷⁵ Art. 46.9 de la Propuesta de REEDS.

⁷⁶ Art. 46.12 de la Propuesta de REEDS.

⁷⁷ Art. 46.11 de la Propuesta de REEDS.

⁷⁸ Art. 46.3 de la Propuesta de REEDS.

⁷⁹ Art. 46.4 de la Propuesta de REEDS.

5.2. Procedimiento simplificado

Aunque el REEDS no le otorga expresamente esta denominación, se trata de un procedimiento simplificado en la medida en que se lleva a cabo sin la intervención de los organismos de acceso y con el fin de aligerar su previsible carga administrativa⁸⁰. Se aplica a aquellos supuestos en que el usuario solicita el acceso a conjuntos de datos de un titular individual y en un único Estado miembro. De cumplirse tal condicionalidad, la petición del usuario podrá dirigirse directamente ante el titular correspondiente, quien será quien sopesa la solicitud y, en su caso, quien conceda el permiso de datos⁸¹.

No obstante, el titular deberá cumplir los requisitos de tiempo y forma generalmente aplicables al procedimiento ordinario, incluyendo el contenido mínimo exigible a las solicitudes y permisos. Esto incluye el plazo máximo de dos meses para responder a la solicitud (prorrogable por otros dos en caso de peticiones complejas) y, concedida aquella y expedido el permiso, de otros dos meses (prorrogables) para poner a disposición del usuario los datos mediante un entorno de tratamiento seguro.

La inclusión de este procedimiento en la versión final de la Propuesta resulta, a día de hoy, incierta, habida cuenta de que diversos agentes se han pronunciado en contra de mantenerlo por los potenciales riesgos de prescindir de la intermediación y supervisión de los organismos de acceso⁸². A nuestro parecer, si bien es cierto que la intervención de los citados organismos constituye un pilar fundamental del REEDS y una garantía del correcto funcionamiento de sus mecanismos de gobernanza, nada impide a estas entidades (o, en su caso, a las autoridades de protección de datos competentes) llevar a cabo un control y monitorización *ex post*, por supuesto, la eventual imposición de sanciones. Es más, para ello precisamente introduce este tipo de procedimiento la obligación de que los titulares informen al organismo de acceso competente, en un plazo máximo de tres meses, de todas las solicitudes de acceso recibidas y, en su caso, de los permisos expedidos⁸³. Ello se alinea, por ende, con las obligaciones de responsabilidad proactiva del RGPD, de suerte que el grado de control del cumplimiento efectivo dependerá, en última instancia, de que los organismos sean dotados de recursos suficientes para el desempeño de tales funciones con la diligencia y eficiencia debidas.

6. Conclusiones

La creación del Espacio Europeo de Datos de Salud por medio de la aprobación de su correspondiente Reglamento (REEDS) pretende erigirse como un importante hito para superar la fragmentación normativa existente, establecer mecanismos de gobernanza comunes y, en suma, impulsar la reutilización de datos de salud en beneficio de la sociedad y del interés general. Se trata de un instrumento de suma complejidad por cuanto regulará una pluralidad de cuestiones interdisciplinarias, debiendo coexistir e interactuarse con la lógica sistemática de normas ya

⁸⁰ Así se infiere de lo dispuesto por el Considerando 53 de la Propuesta de REEDS.

⁸¹ Considerando 53 y art. 49 de la Propuesta de REEDS.

⁸² En este sentido se han pronunciado, entre otros: Committee on the Environment, Public Health and Food Safety & Committee on Civil Liberties, Justice and Home Affairs, *Draft Report on the proposal for a Regulation on the European Health Data Space*, p. 6; y BEUC, *Position paper on the proposed European Health Data Space*, p. 14.

⁸³ Art. 49.4 de la Propuesta de REEDS.

vigentes, tales como el RGPD. El tercer pilar de la Propuesta (Capítulo IV, arts. 33 a 58) se ocupa de los usos secundarios de los datos de salud electrónicos. Por medio del presente artículo se ha acometido un estudio comprensivo de este régimen de acceso a los datos electrónicos de salud para usos secundarios, con especial atención a aquellos de carácter personal. Con ello, se han examinado sus carencias y virtudes y su compleja integración e interacción con la normativa europea de protección de datos de carácter personal, en particular, con el RGPD.

Así, en primer lugar, el régimen propuesto consolida una doble tendencia expansiva con respecto al RGPD. Por un lado, porque el ámbito de aplicación objetivo del REEDS se extenderá tanto a los datos electrónicos personales como a los no personales, confirmándose el viraje hacia un modelo finalista en que los tratamientos de datos pasarían a autorizarse por razón de sus eventuales usos o finalidades; y tratando de solventar, a su vez, la cada vez más difusa dicotomía entre el dato personal y el no personal y/o el dato sensible y el no sensible. Por otro lado, la Propuesta acuña una noción de «datos de salud electrónicos personales» que es conceptualmente más extensa que la de «datos relativos a la salud» empleada por el RGPD, en la medida en que la primera incluye no solo estos últimos, sino también los «datos genéticos» en general; dos categorías especiales de datos, de por sí, abiertas y comprensivas. Como resultado de ello, el texto español de la Propuesta debe ser enmendado a fin de corregir la inoportuna confusión entre los términos en inglés «*health data*» y «*healthcare data*» que equivaldrían a lo que conocemos, respectivamente, como «datos de salud» y «datos sanitarios», de suerte que el último evocaría un ámbito considerablemente más estricto que el realmente pretendido por el legislador.

En segundo lugar, otra compleja interacción es la del concepto de «uso secundario» del REEDS, tradicionalmente ajena a la jerga de la protección de datos personales, con la noción de «tratamiento ulterior» empleada por el RGPD. La categorización de los usos secundarios que realiza la Propuesta es ambigua y, aunque ambas expresiones suelen ser indistintamente invocadas con gran asiduidad, no resultan del todo equiparables. A efectos de protección de datos no cabe hablar de «usos primarios» sino de «tratamiento inicial», ni de «usos secundarios» sino de «tratamientos ulteriores». La interrelación de ambas figuras es compleja y no ha sido abordada en absoluto por el texto del REEDS, por lo que deberá ser, en su caso, acometida por parte de las autoridades de control nacionales o europeas si lo que se pretende es lograr una coexistencia y congruencia interpretativa y aplicativa entre ambos cuerpos normativos.

En tercer lugar, en lo que se refiere a los usos secundarios permitidos, la Propuesta establece taxativamente un total de ocho, que pueden clasificarse en dos grupos bien diferenciados por razón de la naturaleza de los titulares de datos que pueden presentar las solicitudes de acceso a datos. En lo que concierne particularmente a los usos secundarios de investigación científica, el REEDS constituye otra oportunidad legislativa perdida para delimitar con claridad el concepto y los contornos de los fines de «investigación científica», pues se limita a seguir la estela del RGPD enunciando un concepto amplio, pero ambiguo. Como consecuencia de la adopción de la noción comprensiva del RGPD, la mención expresa a los usos secundarios de «actividades de desarrollo e innovación de productos o servicios» y «el entrenamiento, la prueba y la evaluación de algoritmos» debería ser suprimida por encontrarse ya subsumidos en la de «investigación científica» en sentido lato o, en su caso, deberían incluirse a efectos meramente descriptivos e ilustrativos de esta última. Por fin, consideramos que la única forma de que el futuro REEDS responda fielmente a los objetivos para los que ha sido concebido y, a su vez, no termine por menoscabar la confianza de la sociedad en el sistema propuesto, es la articulación de un proceso

transparente y participativo que dé voz a las diferentes partes interesadas a la hora de mantener los usos secundarios permitidos o prohibidos o de introducir cualesquiera otros no previstos.

En cuarto lugar, el REEDS pretende implementar todo un conglomerado de nuevos actores y componentes que deberán interrelacionarse y coexistir con aquellos ya existentes por mor de la normativa de protección de datos personales, incluyendo sus principios, bases de licitud o roles legales. Bajo la designación de *titulares de datos* se agrupa a todo un conjunto de personas físicas o jurídicas, entidades u organismos del sector sanitario o asistencial cuyo elemento aglutinador es la obligación de puesta a disposición para su uso secundario por los usuarios de los datos que así lo soliciten. Por su parte, los *usuarios de datos* que, a diferencia de los titulares, incluyen cualesquiera personas físicas o jurídicas, con independencia del sector en que desarrollen su actividad. En lo que concierne a los *organismos de acceso a datos*, se trata de organismos públicos y/o administrativos con independencia funcional y económica a quienes competirá, 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. Concedido el acceso, usuario y organismos de acceso serán considerados corresponsables del tratamiento hasta la conclusión de las actividades de tratamiento en cuestión. Finalmente, el REEDS instituirá una infraestructura transfronteriza (*HealthData@EU*) que coordinará los diversos nodos federados y organismos de acceso que integren el Espacio y será operada por la Comisión Europea, quien ocupará la posición de encargada del tratamiento. Interesantemente, podrán incorporarse como participantes autorizados a esta plataforma no solo organismos, instituciones, consorcios, repositorios o biobancos de la UE, sino también organizaciones internacionales y nodos u organismos de acceso de terceros países.

En quinta y última instancia, el acceso a datos para usos secundarios en el seno del REEDS se sustanciará por medio de un proceso reglado y común a nivel europeo, previéndose al efecto dos tipos de procedimientos: uno *general*, aplicable a las solicitudes de acceso que impliquen varios conjuntos de datos situados en dos o más Estados miembros y otro *simplificado*, para aquellos supuestos en que un usuario solicite el acceso a datos de un único titular de un solo Estado miembro. La principal diferencia entre ambos procedimientos estriba en que en el primero de ellos la intermediación de uno o más organismos de acceso es obligatoria, mientras que en el simplificado los usuarios podrán presentar sus solicitudes de acceso directamente ante los titulares correspondientes. Si bien es cierto que el hecho de prescindir de la intervención de los organismos de acceso ha suscitado ciertas reticencias, a nuestro parecer, el REEDS establece obligaciones y garantías adecuadas y suficientes y, en cualquier caso, nada impide un control ex post de los permisos concedidos y de los usos secundarios alegados ni, por supuesto, la eventual imposición de sanciones. En definitiva, lo anterior se alinea con el principio de responsabilidad proactiva del RGPD, siendo así que el grado de control del cumplimiento dependerá, en última instancia, de que los organismos de acceso sean dotados de los recursos suficientes para el desempeño de sus funciones de manera efectiva.

7. Bibliografía

ABERASTURI GORRIÑO, Unai, *La protección de datos en la sanidad*, Thomson Reuters Aranzadi, 2013.

ALKORTA IDIAKEZ, Itziar, *El Espacio Europeo de Datos Sanitarios: Nuevos enfoques para la protección e intercambio de datos sanitarios*, Thomson Reuters Aranzadi, 2022.

BECKER, Regina, et. al. «Secondary Use of Personal Health Data: When is it “further processing” under the GDPR and what are the implications for data controllers?», *European Journal of Health Law*, 30(2), 2022, pp. 129 ss.

COTINO HUESO, Lorenzo, «El alcance e interacción del régimen jurídico de los datos personales y big data relacionado con la salud y la investigación biomédica», *Revista de Derecho y Genoma Humano: Genética, Biotecnología y Medicina Avanzada*, 52, 2020, pp. 57 ss.

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 ss.

DE MONTALVO JÄÄSKELÄINEN, Federico, «Ethical and legal requirements for biomedical research involving health data in the context of the COVID-19 pandemic: is informed consent still playing the leading role?», *BioLaw Journal*, Special Issue 2, 2021, pp. 157 ss.

FORGÓ, Nikolaus, «My health data – your research: some preliminary thoughts on different values in the General Data Protection Regulation», *International Data Privacy Law*, 5(1), 2015, pp. 54 ss.

FRANKLIN, Michael et al. «From databases to dataspace: A new abstraction for information management», *SIGMOND Record*, 34, n.º 4, 2005, pp. 28 ss.

HORGAN, Denis, et al., «European Health Data Space – An opportunity now to grasp the future of data-driven healthcare», *Healthcare*, 10(9), 2022.

JOVE VILLARES, Daniel, *La protección de lo sensible o cuando la naturaleza del dato no lo es todo*, Tirant lo Blanch, 2023.

KAPLAN, Bonnie, «How Should Health Data Be Used? Privacy, Secondary Use, and Big Data Sales», *Cambridge Quarterly of Healthcare Ethics*, 25(2), 2016, pp. 312 ss.

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

MARELLI, Luca, et al., «The European Health Data Space: too big to succeed?», *Health Policy*, 135, 104861, 2023.

MARTÍNEZ MARTÍNEZ, Ricard, «Digitalización y construcción normativa de los Espacios Europeos de Datos: retos para el sector público», *La Ley Privacidad*, 13, 2022.

MOLNÁR-GÁBOR, Fruzsina, et al. «Bridging the European Data Sharing Divide in Genomic Science», *Journal of Medical Internet Research*, 24(10), 2022, e37236.

MURILLO DE LA CUEVA, Pablo Lucas, «La publicidad de los archivos judiciales y la confidencialidad de los datos sanitarios», *VII Congreso Nacional de Derecho Sanitario*, Madrid, 2000.

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

NICOLAS, Pilar, «El concepto de dato médico y genético», en RIPOL CARULLA, Santiago (ed.) / BACARIA MARTRUS, Jordi (coord.), *Estudios de protección de datos de carácter personal en el ámbito de la salud*, Marcial Pons, Barcelona, 2006, pp. 77 ss.

QUINN, Paul, «Is the GDPR and Its Right to Data Portability a Major Enabler of Citizen Science?», *Global Jurist*, 18(2), 2018.

QUINN, Paul/MALGIERI, Gianclaudio, «The Difficulty of Defining Sensitive Data – The Concept of Sensitive Data in the EU Data Protection Framework», *German Law Journal*, 22(8), 2022.

RECUERO, Mikel, «El Espacio Europeo de Datos de Salud: retos y oportunidades para la protección de datos de carácter personal», en BUENO DE MATA, Federico (dir.) / GONZÁLEZ PULIDO, Irene (coord.), *Fodertics 10.0: estudios sobre derecho digital*, Comares, Granada, 2022, pp. 389 ss.

RECUERO, Mikel, «La investigación científica con datos personales genéticos y datos relativos a la salud: perspectiva europea ante el desafío globalizado», *Premios de Investigación en Protección de Datos Personales Emilio Aced*, Agencia Española de Protección de Datos, Madrid, 2019.

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

SKOVGAARD, Lea, et al., «A review of attitudes towards the reuse of health data among people in the European Union: the primacy of purpose and the common good», *Health Policy*, 123(6), 2019, pp. 564 ss.

SLOKENBERGA, Santa, «Scientific research regime 2.0? Transformations of the research regime and the protection of the data subject that the proposed EHDS regulation promises to bring along», *Technology and Regulation*, 2022, pp. 135 ss.

STAUNTON, Ciara, et al. «Ethical and social reflections on the proposed European Health Data Space», *European Journal of Human Genetics*, 2024.

TERZIS, Petros, «Compromises and Asymmetries in the European Health Data Space», *European Journal of Health Law*, 30(3), 2022, pp. 345 ss.