EL IMPACTO REGULATORIO Y DE SEGURIDAD DE LA INTEROPERABILIDAD DE LOS DATOS EN EL ÁMBITO SANITARIO: PERSPECTIVAS EN PROTECCIÓN DE DATOS Y CIBERSEGURIDAD

Marc Sabaté Martínez

Consorci de Salut i Social de Catalunya

Claudia Gómez Zaragoza

Consorci de Salut i Social de Catalunya

Daniel Morante Morante

Consorci de Salut i Social de Catalunya

SUMARIO

- I. Introducción.
- II. Regulación que se desprende del nuevo paradigma de interoperabilidad de los datos.
- III. Impacto derivado de la interoperabilidad de los datos en la gestión de la protección de datos.
- IV. Impacto derivado de la interoperabilidad de los datos en la gestión de la ciberseguridad.
- V. Conclusiones.
- VI. Fuentes consultadas.

RESUMEN

Análisis del papel crucial de la nueva perspectiva europea de interoperabilidad de datos en el ámbito sanitario, así como sus implicaciones frente a la normativa vigente. Se examina el modo en que la interoperabilidad incide e incidirá en la gestión de la protección de datos, resaltando la imperiosa necesidad de preservar la confidencialidad y la integridad de la información médica. Además, se indaga en el impacto sobre la ciberseguridad, haciendo hincapié en la pertinencia de implementar medidas específicas para mitigar posibles vulnerabilidades y ataques, en aras de asegurar una interoperabilidad que sea tanto eficaz como segura en el contexto sanitario.

PALABRAS CLAVE

Interoperabilidad de datos, ámbito sanitario, protección de datos, ciberseguridad, confidencialidad, integridad.

ABSTRACT

Analysis of the crucial role of the new European perspective on data interoperability in the healthcare sector, as well as its implications with respect to current regulations. It examines how interoperability affects and will affect data protection management, emphasizing the urgent need to preserve the confidentiality and integrity of medical information. Furthermore, it investigates the impact on cybersecurity, emphasizing the relevance of implementing specific measures to mitigate potential vulnerabilities and attacks, in order to ensure interoperability that is both effective and secure in the healthcare context.

KEYWORDS

Data interoperability, healthcare sector, data protection, cybersecurity, confidentiality, integrity.

I. INTRODUCCIÓN

En un mundo donde la innovación tecnológica está redefiniendo los límites de la atención médica, la interoperabilidad de los sistemas de datos emerge como una innovación tecnológica y organizativa revolucionaria con el potencial de redefinir la práctica clínica y la gestión de la salud a nivel global.

Durante mucho tiempo los sistemas de salud han hablado distintas lenguas, y esto dificulta enormemente la comunicación e interacción entre los mismos. Es por este motivo que desde las instituciones europeas se aboga por un paradigma que gire entorno a la interoperabilidad de los sistemas en el sector sanitario con la finalidad de aumentar la seguridad de los usuarios permitiendo el acceso y la disponibilidad de los datos clínicos; por lo que debería ser un imperativo establecer mecanismos que faciliten el intercambio de información entre los distintos sistemas de salud. La Comisión, adaptó en 2010 una comunicación titulada “Hacia la interoperabilidad de los servicios públicos europeos” que comprende la Estrategia Europea de Interoperabilidad (EIS) y el Marco Europeo de Interoperabilidad (EIF). Se considera que, desde entonces, el Marco Europeo de Interoperabilidad ha servido de referencia de toda la Unión y fuera de ella, constituyendo la base de la mayoría de los marcos nacionales de la interoperabilidad y sus estrategias¹.

La presente comunicación realizará una aproximación al impacto que se prevé que pueda tener el nuevo paradigma de la interoperabilidad de datos sanitarios a nivel europeo respecto a la protección de datos y a la seguridad de los sistemas de información. Para ello, se tomarán como base las legislaciones propias de protección de datos y referentes a la ciberseguridad a nivel europeo y a escala nacional, además de las citadas normativas, el análisis versará también alrededor de la propuesta del nuevo Espacio Europeo de Datos Sanitarios (EEDS). De acuerdo a la mencionada propuesta de Reglamento del nuevo EEDS y completando la definición dada por el Marco Europeo de Interoperabilidad, se entiende por interoperabilidad la capacidad de las aplicaciones o dispositivos informáticos del mismo fabricante o de diferentes fabricantes, para interactuar con fines mutuamente beneficiosos, que consista en un intercambio de información y conocimientos que no modifique el contenido de los datos entre estas organizaciones, aplicaciones o dispositivos informáticos, a través de los procesos a los que dan apoyo.

¹ Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. (2017). Marco Europeo de Interoperabilidad – Estrategia de aplicación.

Con este análisis se pretende aportar una visión breve realizada des del Consorci de Salut i d'Atenció Social de Catalunya alrededor de que regulaciones se verán afectadas por el inminente nuevo paradigma del espacio europeo de datos compartidos y qué acercamientos deberán de llevarse a cabo en cuanto a la protección de los datos sanitarios y la seguridad de estos. La estructura seguida durante la comunicación, se vertebra entre una primera toma de contacto con las normativas ya mencionadas en la presente introducción, seguida de un análisis breve a nivel de las implicaciones de este nuevo espacio en el sistema sanitario actual, y que acciones deberán tomarse para garantizar la integridad, disponibilidad y confidencialidad del dato.

II. REGULACIÓN QUE SE DESPRENDE DEL NUEVO PARADIGMA DE INTEROPERABILIDAD DE LOS DATOS

Los inicios de la regulación reciente europea en la materia se remontan a la Estrategia Europea de Interoperabilidad (EIS) y al Marco Europeo de Interoperabilidad (EIF). En este último (referente común para las normas venideras), la UE garantizaba la interoperabilidad jurídica, organizativa, semántica y técnica bajo la siguiente perspectiva: “Las administraciones públicas habrán de facilitar servicios públicos digitales interoperables clave con primacía del usuario a empresas y ciudadanos, a escala nacional y de la Unión, fomentando la libre circulación de bienes, personas, servicios y datos en toda la Unión”². En consonancia con su misión, el EIF definió las directrices básicas de interoperabilidad mediante principios fundamentales, modelos y recomendaciones comunes.

En la actualidad, la Estrategia Europea de Datos busca convertir a la Unión en líder de una sociedad basada en los datos, mediante la creación de un mercado único de datos que permitirá que estos fluyan libremente por la Unión y entre sectores, en beneficio de las empresas, el personal investigador y las Administraciones Públicas³. El primer resultado de la estrategia se trata del Reglamento de Gobernanza de Datos⁴, aplicable desde septiembre de 2023, que

² Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. (2017): Marco Europeo de Interoperabilidad – Estrategia de aplicación.

³ Comisión Europea. (2019): «Estrategia Europea de datos»: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_es

⁴ Reglamento (UE) 2022/868 del Parlamento Europeo y del Consejo, de 30 de mayo de 2022 relativo a la gobernanza europea de datos y por el que se modifica el Reglamento (UE) 2018/1724 (Reglamento de Gobernanza de Datos).

ha sido complementado por el Reglamento sobre normas armonizadas sobre el acceso y el uso equitativo de los datos⁵ (Reglamento de Datos), ya en vigor y aplicable a partir de septiembre de 2025. Si bien el Reglamento de Gobernanza de Datos regula los procesos y estructuras que facilitan el intercambio voluntario de datos, el Reglamento de Datos aclara quién puede crear valor a partir de los datos y en qué condiciones⁶. También recientemente ha sido aprobado el “Reglamento sobre la Europa Interoperable”⁷, que resulta la máxima expresión de la interoperabilidad en el sector público de la UE. En él se establecen medidas que fomentan la interoperabilidad transfronteriza de los servicios públicos digitales transeuropeos, contribuyendo así a la interoperabilidad de los sistemas de redes y de información subyacentes mediante el establecimiento de normas comunes y un marco de gobernanza. Como anuncia en su treceavo considerando, “considerar la interoperabilidad por sectores conlleva el riesgo de que (...) surjan nuevas barreras electrónicas que dificulten el correcto funcionamiento del mercado interior y las libertades de circulación que trae consigo”, por lo que facilita la interoperabilidad intersectorial, apoyando la eliminación de dichas barreras, incompatibilidades y fragmentación de los servicios públicos digitales. Este Reglamento surge a colación de qué evaluaciones recientes habían puesto de manifiesto que el enfoque de cooperación voluntario establecido por el EIF ostentaba graves limitaciones⁸. De este modo, se prevé la creación del Comité de la Europa Interoperable, en el que se le asignan diversas funciones, entre ellas, la de desarrollar el Marco Europeo de Interoperabilidad, así como su actualización (artículos 6 y 5).

En este contexto, la interoperabilidad de los datos en el ámbito sanitario se desarrolla en la *Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el Espacio Europeo de Datos Sanitarios*. El EEDS constituye la primera propuesta de ámbito específico de espacio común europeo, en desarrollo de la Estrategia Europea de Datos mencionada anteriormente. Su objetivo principal es garantizar que las

personas físicas de la UE tengan un mayor control en la práctica sobre sus datos sanitarios electrónicos, aunque también tiene por objeto: a) “garantizar un marco jurídico consistente en mecanismos de gobernanza fiables de la UE y de los Estados miembros y un entorno de tratamiento seguro para mejorar el diagnóstico, tratamiento, y bienestar de las personas, además de dar lugar a políticas mejores y bien informadas”; y b) “contribuir a un auténtico mercado único de productos y servicios sanitarios digitales, y armonizar las normas para impulsar la eficiencia de los sistemas sanitarios”⁹. Así pues, atendiendo a su objetivo y objeto de regulación, la interoperabilidad de los datos sanitarios es el fundamento del EEDS: promueve un mejor intercambio y acceso a diferentes tipos de datos sanitarios electrónicos, y apoya tanto el uso primario de los datos sanitarios electrónicos como su uso secundario y las actividades de cesión altruista de estos datos.

Por su parte, el Reglamento del EEDS reconoce encontrarse en coherencia con el resto de normativa existente: siendo diseñado de conformidad con el RGPD, el Reglamento de protección de datos de la UE¹⁰, los Reglamentos sobre productos sanitarios¹¹, la propuesta de Reglamento de Inteligencia Artificial¹² e innova respecto a la Directiva sobre asistencia sanitaria transfronteriza¹³. En lo que se refiere a las previsiones sobre el uso secundario de datos electrónicos, se basa en los ya mencionados Reglamento de Gobernanza de Datos y Reglamento de Datos, complementándolos y estableciendo normas más específicas para el sector sanitario. Se basa igualmente en la Directiva SRI II o NIS II¹⁴,

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

6 Ley de datos. «Configurar el Futuro Digital de Europa». <https://digital-strategy.ec.europa.eu/es/policies/data-act>

7 Reglamento (UE) 2024/903 del Parlamento Europeo y del Consejo, de 13 de marzo de 2024, por el que se establecen medidas a fin de garantizar un alto nivel de interoperabilidad del sector público en toda la Unión.

8 Reglamento sobre la Europa Interoperable: el Consejo adopta un nuevo Reglamento para unos servicios públicos digitales más eficientes en toda la UE». <https://www.consilium.europa.eu/es/press/press-releases/2024/03/04/interoperable-europe-act-council-adopts-new-law-for-more-efficient-digital-public-services-across-the-eu/>

9 Propuesta de Reglamento del Parlamento Europeo y del Consejo, sobre el Espacio Europeo de Datos Sanitarios.

10 Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) n.º 45/2001 y la Decisión n.º 1247/2002/CE.

11 Reglamento (UE) 2017/745 del Parlamento Europeo y del Consejo, de 5 de abril de 2017, sobre los productos sanitarios, y Reglamento (UE) 2017/746 del Parlamento Europeo y del Consejo, de 5 de abril de 2017, sobre los productos sanitarios para diagnóstico in vitro.

12 Propuesta de Reglamento por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial).

13 Directiva 2011/24/UE del Parlamento Europeo y del Consejo, de 9 de marzo de 2011, relativa a la aplicación de los derechos de los pacientes en la asistencia sanitaria transfronteriza.

14 Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) n.º 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148.

respecto a las normas de ciberseguridad en la UE, con intención de reforzar la seguridad y la confianza en el marco técnico diseñado para facilitar el intercambio de datos sanitarios (tanto para su uso primario como secundario).

En España, la interoperabilidad de los datos se establece como uno de los principios de actuación de las Administraciones Públicas en el art. 3 de la Ley 40/2015, que a su vez su recoge al Esquema Nacional de Interoperabilidad (ENI) en su art. 156. Por su parte, la regulación del ENI se encuentra en el Real Decreto 4/2010, de 8 de enero, viniendo establecido por el art. 42 de la Ley 11/2007. El ENI dispone tres principios específicos: la interoperabilidad como cualidad integral, el carácter multidimensional de la interoperabilidad, y el enfoque de soluciones multilaterales. A raíz del ENI se desarrollan las normas técnicas de interoperabilidad entre las Administraciones Públicas (para las que resultan de obligado cumplimiento) y los ciudadanos. Aún vigente, el ENI sólo ha sido modificado en una ocasión: por el Real Decreto 203/2021, de 30 de marzo por el que regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica. Al respecto, la aplicación de la interoperabilidad en el ámbito sanitario se fundamenta en la Ley 16/2003, de cohesión y calidad del Sistema Nacional de Salud (SNS), en el que se ordena al Ministerio de Sanidad el desarrollo de los sistemas de tarjeta sanitaria y de intercambio de la información clínica y de receta electrónica en el SNS. Asimismo, la Estrategia de Salud Digital del SNS (2021-2026) prevé entre sus líneas de actuación la generalización de la interoperabilidad de la información sanitaria. Un ejemplo ilustrativo de la Estrategia podría ser el *Real Decreto 572/2023, de 4 de julio, por el que se modifica el Real Decreto 1093/2010, de 3 de septiembre, por el que se aprueba el conjunto mínimo de datos de los informes clínicos en el SNS*, pues esta modificación tiene como objetivo exclusivo contribuir a la mejora de la interoperabilidad de los informes clínicos que se producen en el SNS.

Debe resaltarse el proyecto por el que se crea el Espacio Nacional de Datos de Salud (ENDS) o también llamado “Data Lake Sanitario” cuya finalidad pretende “que recoja la información procedente de los diferentes sistemas de información autonómicos, permitiendo su análisis masivo para la identificación y mejora de diagnósticos y tratamientos”¹⁵.

15 Consejo de Ministros (2022): «El Gobierno aprueba la distribución territorial de 28 millones de euros de fondos europeos para el desarrollo de un Espacio Nacional de Datos de Salud». Nota de prensa. Ministerio de Asuntos Económicos y Transformación Digital, págs. 1 y 2 (https://portal.mineco.gob.es/RecursosNoticia/mineco/prensa/noticias/2022/20221220 NDP_distribuci%C3%B3n_inversi%C3%B3n_data_lake_sanitario.pdf).

La Secretaría de Estado de Digitalización e Inteligencia Artificial es la responsable del proyecto, actuando a través de la Secretaría General de Administración Digital en colaboración con el Ministerio de Sanidad y el conjunto de comunidades y ciudades autónomas de España, todo ello con el apoyo del Ministerio de Transformación Digital y Función Pública. El proyecto se encuentra financiado por la Unión Europea, pues forma parte del Plan de Recuperación, Transformación y Resiliencia (Next Generation EU): el pasado 20 de diciembre de 2022 ya se destinaron 28 millones de euros a este propósito, aunque al tiempo de redactar esta comunicación el ENDS se encuentra estancado en el procedimiento de licitación. Sin lugar a duda, el objeto del ENDS recae en el uso secundario de los datos, y se encuentra en consonancia con lo estipulado en la Disposición adicional decimoséptima sobre tratamientos de datos de salud de la LOPDGDD. Asimismo, en aras del desarrollo del futuro EEDS, el ENDS debe asegurar un nivel de servicio, los estándares de anonimización o seudonimización, la interoperabilidad y la seguridad de la información¹⁶.

En Cataluña, desde hace tiempo se promueven medidas para facilitar la interoperabilidad en las Administraciones Públicas, como el Convenio Marco de Colaboración de 2006¹⁷. Posteriormente, la ley 29/2010, de 3 de agosto, recogió el marco de interoperabilidad del sector público de Cataluña (siendo el instrumento por el que se dota al sector público de Catalunya para garantizar los niveles necesarios de interacción e integración en los aspectos tecnológicos, semánticos y organizativos de sus procesos, mediante el uso intensivo de las tecnologías de la información y la comunicación). La interoperabilidad de los datos sanitarios encuentra su cabida en la “historia clínica compartida”, a la que acceden tanto los profesionales del sistema sanitario catalán como los pacientes (cuando se trate de su documentación médica personal), y creada por la *Ley 16/2010, de 3 de junio, de modificación de la Ley 21/2000, de 29 de diciembre, sobre los derechos de información concerniente a la salud y la autonomía del paciente, y la documentación clínica*.

16 Portal de la Administración Electrónica. (2024): «El Espacio Nacional de Datos de Salud: un proyecto estratégico para España» (https://administracionelectronica.gob.es/pae/Home/pae_Actualidad/pae_Noticias/2024/Abril/noticia-2024-04-19-Espacio-Nacional-Datos-Salud-proyecto-estrategico-.html)

17 *Conveni Marc de Col·laboració entre el Departament de Governació i administracions públiques, en nom de l'administració de la Generalitat de Catalunya, el Consorci LOCALRET, l'Ajuntament de Barcelona i el Consorci d'Administració Oberta Electrònica de Catalunya per a l'impuls i el desenvolupament de la interoperabilitat dels sistemes d'informació de les administracions catalanes*, de 22 de octubre de 2006.

El paradigma regulatorio expuesto sobre la interoperabilidad de los datos en sede europea, estatal y autonómica resulta de gran alcance y ambición. Si bien es cierto que nos dirigimos hacia un modelo de interoperabilidad transversal, pues se concibe que el tratamiento de los datos será regulado por normas comunes para evitar la fragmentación y derribar barreras para los servicios públicos que sean transversales (como dispone el Reglamento sobre la Europa Interoperable), no es menos cierto la interoperabilidad de los datos también estima su propia regulación por sectores para que resulte efectiva, que en el caso de la salud se plasma en el EEDS en Europa, el desarrollo del ENDS en España y mediante la HC3 en el caso de Cataluña. Es por ello por lo que, si bajamos otro escalón en esta pirámide normativa, encontramos el instrumento que contribuye a hacer efectiva la deseada interoperabilidad: los códigos de conducta, regulados en los arts. 40 y 41 RGPD. Éstos cobran especial relevancia pues, vista toda la regulación que es aplicable en las distintas esferas, materializan todos aquellos deberes y obligaciones que debe seguir el tratamiento de los datos en cada sector, según sea su ámbito de aplicación, pudiendo ser de alcance nacional o transnacional -si los códigos de conducta guardan relación con actividades de tratamiento en varios Estados miembros de la Unión Europea. Contar con la adhesión a un código de conducta es el primer paso para que las entidades, instituciones y organizaciones garanticen el cumplimiento del RGPD y LOPDGDD. Asegurar que los tratamientos de los datos son conformes a la legislación de protección de datos desde el más bajo nivel (entendido como el punto de partida) resulta crucial para que la construcción de los niveles superiores sea posible, y llegue a culminarse de forma efectiva el anhelado EEDS.

En el sector que nos atañe es de obligada mención el Código de Conducta para el tratamiento de datos personales en el ámbito sanitario, que fue promovido por el Consorci de Salut i d'Atenció Social de Catalunya y aprobado por la Autoridad Catalana de Protección de Datos (APDCAT) el 22 de diciembre de 2020, mediante la resolución Ref. CC 1/2020. Como es sabido, las entidades que se adhieren a un código de conducta dan cumplimiento al principio de "responsabilidad proactiva" del art. 5.2 RGPD en aplicar sus disposiciones, por lo que este instrumento garantiza que dichas entidades sean capaces de demostrar la conformidad del tratamiento de los datos con la normativa sectorial aplicable (véase art. 111-1). Su ámbito de aplicación ostenta dos vertientes: la objetiva, que es la creación de un marco común y la unificación en criterios en la aplicación de la normativa de protección de datos en el sector sanitario, y la subjetiva, que pretende su aplicación para las diversas entidades que forman

parte del sistema sanitario integral de utilización pública de Cataluña (SISCAT) y, si procede, las entidades que les prestan servicios (véase art. 112.2). Dicho Código se articula en base a la problemática propia que pueden presentar los tratamientos de datos personales en el ámbito de la salud, y se centra en los aspectos que pueden generar más dudas a las entidades en relación con el tratamiento de los datos que les competen. Todo ello de acuerdo con las directrices 1/2019¹⁸, en las que se establece que los titulares del código deben demostrar la correcta aplicación del RGPD, con una serie de requisitos, lo que queda plasmado en el propio Código y en su Memoria de elaboración pues éste dispone que *"El objetivo principal es desarrollar mecanismos que permitan aplicar de manera específica la normativa en materia de protección de datos existente a nivel europeo y nacional, para intentar dotarla de unos criterios específicos claros que sirvan de guía de buenas prácticas entre los diferentes actores del sector salud y que al mismo tiempo, garanticen en el ámbito del tratamiento de datos de salud unos estándares de seguridad y un estricto cumplimiento de la legislación"*.

III. IMPACTO DERIVADO DE LA INTEROPERABILIDAD DE LOS DATOS EN LA GESTIÓN DE LA PROTECCIÓN DE DATOS

La protección de datos en el ámbito sanitario se vuelve crucial debido a la delicadeza de la información médica. En España, el manejo de datos sanitarios está sujeto a normativas especiales y citadas anteriormente. Además, hay otras leyes complementarias como pueden ser la Ley 41/2002 de Autonomía del Paciente, que también disponen preceptos acerca de la protección de datos en cuanto a acceso a historias, conservación de documentación, etc.

Los datos sanitarios son considerados sensibles y requieren un nivel de protección más elevado. Esto implica restricciones adicionales en su registro, almacenamiento y procesamiento. En el ámbito sanitario, es fundamental garantizar la confidencialidad y la integridad de la información médica, lo que implica implementar medidas técnicas y organizativas adecuadas para proteger los datos contra accesos no autorizados, pérdidas o alteraciones. Aunque la interoperabilidad puede mejorar la calidad de la atención médica y la eficiencia operativa, también plantea desafíos importantes en cuanto a protección de datos. Esto se debe a que implica la transferencia de datos entre diferentes sistemas, aumentando el

18 European Data Protection Board (2019): Directrices 1/2019 sobre códigos de conducta y organismos de supervisión con arreglo al Reglamento (UE) 2016/679.

riesgo de exposición a amenazas de seguridad. Por lo tanto, como veremos en el apartado cuarto de este mismo artículo, es esencial implementar medidas sólidas en seguridad de la información y ciberseguridad.

Por otro lado, el Reglamento (UE) 2016/679 restringe la portabilidad de datos sanitarios, lo que destaca la necesidad de un enfoque compartido entre los estados miembros y el acceso adecuado por parte de los profesionales sanitarios, manteniendo la seguridad y los derechos de los ciudadanos. Este enfoque compartido se pretende llevar a cabo mediante un ecosistema y a través de la interoperabilidad de los datos en el Espacio Europeo de Datos Sanitarios. Para llevar a cabo este proyecto, se elabora la Propuesta de Reglamento sobre el Espacio Europeo de Datos Sanitarios.

Esta propuesta pretende regular y establecer un marco normativo que permita la interoperabilidad y el intercambio seguro de datos sanitarios entre los países miembros de la Unión Europea. Para lograr esto, la propuesta establece requisitos y estándares para la recopilación, almacenamiento, procesamiento y transferencia de datos sanitarios. También busca garantizar la seguridad y la privacidad de estos datos, mediante la implementación de medidas técnicas y organizativas adecuadas. Con este objetivo, en 2022 se lleva a cabo una evaluación de impacto. Esta sugiere y analiza diversas formas de lograr la interoperabilidad. La opción que más se ajusta a los estándares actuales es una intervención de “intensidad media”, que busca basar la gobernanza en organismos nacionales a nivel nacional y apoyar el desarrollo de requisitos adecuados a nivel de la Unión Europea. Aun así, se presentan tres opciones diferentes basadas en marcos legislativos existentes, con diferencias en flexibilidad y permisividad de los sistemas.

Las tres opciones¹⁹ regulan el uso primario de los datos sanitarios, que se recopilan, almacenan y, en muchos casos, intercambian actualmente. Esto se lleva a cabo mediante conexiones encriptadas punto a punto o a través de sistemas nacionales, con el objetivo de beneficiar a más europeos con diagnósticos y tratamientos más eficientes. Bajo las opciones segunda y tercera, se prohíbe el bloqueo de información por parte de proveedores de atención médica y servicios digitales sanitarios, estableciendo requisitos mínimos de seguridad de datos y asegurando que el intercambio transfronterizo de datos sanitarios se realice de manera segura.

El EEDS se apoya en la Ley de Gobernanza de Datos (DGA) para establecer requisitos y supervisar el uso seguro de los datos sanitarios. La propuesta legislativa establece salvaguardias legales, reglas de minimización de datos y requiere entornos de procesamiento seguro. Se impondrán medidas de seguridad para proteger los datos sanitarios almacenados. El Proyecto establece definiciones claras sobre el uso primario de datos sanitarios electrónicos, incluyendo información sobre salud, datos genéticos y factores determinantes de la salud, tratados en formato electrónico. Aunque la Directiva 2011/24/UE fue pionera en abordar la sanidad electrónica en la UE, su implementación enfrentó obstáculos como la voluntariedad de sus disposiciones y la falta de interoperabilidad entre los sistemas informáticos de salud de los Estados miembros. La Propuesta busca revertir esta situación garantizando el acceso de las personas a sus datos sanitarios electrónicos y la capacidad de los profesionales sanitarios para acceder a la información de los pacientes independientemente de su país de afiliación o de tratamiento.

Los artículos 3 y 4 de la Propuesta establecen el derecho de las personas a acceder a sus datos sanitarios electrónicos y el acceso de los profesionales sanitarios a esta información, respectivamente. Este enfoque garantiza el intercambio de datos entre pacientes y profesionales sanitarios, superando las limitaciones del derecho a la portabilidad de datos establecido en el RGPD. El nuevo EEDS aspira a facilitar el acceso universal a la información sanitaria de los pacientes en la UE, promoviendo la libertad de movimientos entre los Estados miembros. Para lograrlo, se propone un sistema armonizado y seguro de intercambio de datos sanitarios primarios, que incluye la designación de puntos de contacto nacionales para la salud digital en cada Estado miembro. Estos puntos de contacto estarán interconectados a través de una plataforma central para facilitar el intercambio transfronterizo de información sanitaria, garantizando la seguridad y la homologación de los datos. En resumen, la Propuesta busca establecer un marco robusto y coordinado que promueva el acceso equitativo a la información sanitaria y facilite la prestación de servicios de salud transfronterizos en la Unión Europea.

En cuanto al uso secundario²⁰ de datos sanitarios electrónicos, se define como el tratamiento de estos datos para una serie de propósitos detallados en el artículo 34 de la Propuesta, incluyendo actividades de interés público en salud pública, investigación científica, desarrollo e innovación, entre otros. Al

19 European Commission (2022): Commission staff working document executive summary of the impact assessment report 2022. Europa, p. 1.

20 GARCÍA, F. J. (2023): «Introducción al espacio europeo de datos sanitarios: un nuevo horizonte en la gobernanza de datos sanitarios en la unión europea». *Actualidad Jurídica Uriá Menéndez*, p. 187.

igual que con el uso primario de datos, los Estados miembros designarán puntos de contacto nacionales para el uso secundario de datos sanitarios electrónicos, conectados a través de una plataforma central. Además, se designarán organismos de acceso a los datos sanitarios, responsables de conceder acceso a estos datos para uso secundario.

La iniciativa de interoperabilidad del Espacio Europeo de Datos Sanitarios (EEDS) representa un paso significativo en el panorama de la salud europea. Al abordar la interoperabilidad, se enfrenta a desafíos que los Estados miembros no pueden resolver por sí solos. Esta realidad se evidencia en la evaluación²¹ del artículo 14 de la Carta de los Derechos Fundamentales de la Unión Europea (CBHD), que destaca la necesidad de una acción coordinada a nivel supranacional. La opción preferida para regular la gestión y acceso a los datos en el contexto del Espacio Europeo de Datos Sanitarios (EEDS) se presenta como una solución equilibrada y mesurada ante los desafíos que implica la interoperabilidad de los datos Sanitarios en Europa que se evalúa como “proporcionada”, destacando que logra un equilibrio entre diferentes consideraciones, evitando ser demasiado restrictiva o demasiado laxa en sus disposiciones.

IV. IMPACTO DERIVADO DE LA INTEROPERABILIDAD DE LOS DATOS EN LA GESTIÓN DE LA CIBERSEGURIDAD

En la actualidad, el sector salud en Europa se postula como uno de los sectores más vulnerables a los ciberataques, constituyendo el 8% de los incidentes de ciberseguridad reportados. Este porcentaje sitúa al sector sanitario como el segundo más afectado, únicamente superado por la Administración Pública, la cual registra el 19% de los ataques. Esta tendencia contrasta con el resto de los sectores relevantes, como por ejemplo el sector del transporte o sector bancario, ambos con una incidencia del 6%, así como el sector alimentario que representa tan solo el 1%, o el sector educativo impactado con un 4% de los incidentes²². En este contexto, se evidencia la imperiosa necesidad de implementar medidas robustas de ciberseguridad en todas las entidades del ámbito sanitario para mitigar riesgos y proteger la integridad de los sistemas de información, y por tanto la salud y seguridad de los ciudadanos europeos; así como también reducir costes. Trasladando estas cifras a escala nacional, según

datos de INCIBE, en 2022 más de 500 instituciones reportaron incidentes, lo que supone un incremento del 48% respecto al año anterior, y el 89% de las organizaciones sufrieron un intento de ataque Ransomware, el 72% fue perpetrado con éxito²³. Los datos expuestos delimitan un panorama futuro caracterizado por un incremento tanto de la frecuencia como de la sofisticación de los ataques cibernéticos, impulsados en gran medida por el desarrollo y uso de las herramientas de inteligencia artificial. Sin embargo, este contexto alarmante se ve exacerbado por la falta de adecuación de los sistemas de seguridad a las demandas actuales. De hecho, conforme a la publicación de la Agencia Europea de Ciberseguridad previamente referenciada, se revela que el principal vector de ataque en el sector salud, representando el 68% de los casos, trata de una configuración deficiente de las medidas de seguridad. Esta situación se ve complementado por los errores humanos en la operación, constituyendo el 16% de los vectores de ataque identificados. En consecuencia, resulta imperativo abordar de manera urgente las deficiencias en la configuración de la seguridad y fortalecer los sistemas dentro del ámbito sanitario.

En este nuevo paradigma del Espacio Europeo de Datos Sanitarios uno de los mayores riesgos que del mismo se desprenden, son aquellos casos en los que se compromete la integridad, confidencialidad o integridad de los datos de una entidad del sector, no se vería afectada únicamente esta entidad, sino que la interoperabilidad comprometería al resto de entidades que dependen del propio sistema. En respuesta a esta preocupación la propuesta de Reglamento se erige como medida regulatoria integral, incorporando disposiciones de diversas normativas previamente mencionadas en el apartado segundo de la presente comunicación y un incluyendo un anexo específico que detalla los requisitos de seguridad. El propósito fundamental de esta iniciativa es establecer estándares uniformes y requisitos mínimos para la participación en dicho espacio, buscando así salvaguardar la integridad y confidencialidad de los datos sanitarios en el ámbito europeo.

Uno de los grandes interrogantes que se cierne sobre el nuevo espacio de datos es como se regulará a nivel de seguridad. En el ámbito nacional la regulación recae sobre el Esquema Nacional de Seguridad cuya finalidad es la creación de las condiciones necesarias de confianza en el uso de los medios electrónicos a través de medidas para garantizar la seguridad de los sistemas²⁴. El panorama del cum-

21 European Commission (2022): Commission staff working document. Impact Assessment Report 2022. Europa, p.3.

22 European Union Agency for Cybersecurity (2023): ENISA THREAT LANDSCAPE 2023. Europa. ENISA, p. 13

23 Digital Eye Observatory (2023): «La e-pandemia. Ataques al sector sanitario». Digital Eye.

24 MUÑOZ, L. y GALLEGOS, S. (2019): «La protección de datos y la interoperabilidad en el ámbito sanitario: dos realidades inseparables». *Derecho y Salud*, Volumen 29, p. 39.

plimiento normativo en el Esquema Nacional de Seguridad presenta cifras preocupantes. En el territorio español la certificación bajo este esquema es alarmantemente bajo, reflejando una escasa adhesión a las especificaciones de seguridad establecidas por el esquema. Es importante destacar que la ausencia de certificación no necesariamente indica un incumplimiento de las normativas de seguridad, sin embargo, la obtención de la certificación aporta un valor añadido significativo a la entidad, evidenciando su compromiso con la protección de datos y la seguridad de la información.

La reciente publicación del informe “ENISA Threat Landscape 2023” por parte de la Agencia de la Unión Europea para la Ciberseguridad ofrece un análisis exhaustivo de las tendencias en el ámbito de la ciberseguridad, destacando las amenazas, los actores involucrados, las vulnerabilidades existentes identificadas y los sectores con un mayor impacto. Entre los puntos destacados que aborda esta comunicación, se subraya el significativo aumento del Ransomware, la profesionalización de los actores del ciberdelito y el creciente refinamiento de las técnicas de ingeniería social. Ante este horizonte desafiante, la estrategia nacional de ciberseguridad en España para el año 2023, según lo establecido en el informe del CCN-CERT, se fundamenta en varios pilares clave. Entre ellos se incluyen un marco normativo fortalecido, fomentando así un entorno regulatorio más robusto y adaptado a las nuevas amenazas; la promoción de la cooperación internacional y público-privada para una respuesta más efectiva y coordinada ante los ciberataques; el impulso de desarrollos en ciberseguridad, incentivando la innovación y la adopción de tecnologías avanzadas para la protección de infraestructuras críticas; y el fomento de la concienciación y formación en materia de ciberseguridad, buscando elevar el nivel de preparación y respuesta de todos los actores involucrados en el ecosistema digital. Estos pilares estratégicos se erigen como pilares fundamentales en la gestión proactiva de los riesgos cibernéticos en España.

Desde la perspectiva del Consorci de Salut i d'Atenció Social de Catalunya, se identifica una brecha significativa en la preparación de un ecosistema sanitario para abordar de manera efectiva tanto la prevención como la respuesta ante un proyecto de la envergadura planteada desde Europa. Aunque las principales entidades sanitarias de la comunidad cuentan con recursos económicos, técnicos y organizativos que les permiten disponer de sistemas robustos y seguros, las entidades más pequeñas, que también tendrán acceso al Espacio Europeo de Datos Sanitarios (EEDS), carecen en su mayoría de estas medidas de seguridad, convirtiéndose así en posibles blancos como puerta de entrada al sistema

HME²⁵ debido a su menor resistencia. Con el propósito de equiparar la protección entre todas las entidades del sistema sanitario, la Agencia de Ciberseguretat de Catalunya está desarrollando un modelo de ciberseguridad destinado a todas las entidades integrantes del Sistema Sanitari Integral d'Utilització Pública (SISCAT). Este enfoque busca fortalecer la seguridad cibernética en todas las instancias del sistema sanitario catalán, garantizando así una protección uniforme y efectiva contra las amenazas cibernéticas emergentes; con la finalidad de poder garantizar el cumplimiento de los requisitos generales, los requisitos de interoperabilidad y los de seguridad que se exponen en la propuesta de reglamento del Espacio Europeo de Datos Sanitarios.

En el contexto nacional, la falta de interoperabilidad de los datos sanitarios se presenta como un obstáculo significativo, tanto a nivel interregional como entre los sectores público y privado dentro de una misma comunidad autónoma. La transición hacia un sistema de historial médico electrónico, que anteriormente se consideraba iniciativa de escala autonómica con alcance exclusivo en el sector público, ahora adquiere una dimensión europea que abarca tanto a entidades públicas como privadas. Joaquín Cayon, director del Grupo de Investigación en Derecho Sanitario y Bioética de IDIVAL-Universidad de Cantabria, señala que la reticencia de las distintas instituciones a compartir datos en el ámbito de la asistencia sanitaria ha estado a menudo arraigada en el temor a la responsabilidad derivada de un conocimiento jurídico insuficiente y falta de certeza sobre cómo puede y debe hacerse. En el mismo sentido se expresa Pedro Luis Sánchez, director del departamento de Estudios de FarmaIndustria, afirmando que, en términos absolutos, todavía estamos lejos de los que necesitamos para hacer realidad plenamente el EEDS en el futuro, pero comparando la situación de España con la de otros países de Europa el punto de partida es favorable²⁶.

V. CONCLUSIONES

Visto el marco normativo se concluye que, de un tiempo a esta parte, el legislador europeo usa el reglamento como instrumento para asegurar la homogénea y directa aplicación de sus disposiciones por los Estados Miembros. Tal y como explica la

²⁵ Todo aparato o programa informático destinado por el fabricante a ser utilizado para almacenar, intermediar, importar, exportar, convertir, editar o visualizar historiales médicos electrónicos.

²⁶ EIT Health (2024): «España está en condiciones de liderar en Europa la implementación del EEDS». <https://eithealth.eu/news-article/espana-esta-en-condiciones-de-liderar-en-europa-la-implementacion-del-eesd/?lang=es>

exposición de motivos del Reglamento EEDS, que los derechos de los pacientes en la asistencia sanitaria transfronteriza vengan reconocidos en la Directiva 2011/24/UE (art. 14) con carácter voluntario menoscaba la eficacia de su finalidad, lo que quedó plasmado en la evaluación de impacto que acompaña dicho Reglamento. Esta limitada eficacia de la Directiva se puso igualmente de relieve durante la pandemia de COVID-19, en la que se manifestó la importancia de contar con un alto grado de interoperabilidad y armonización. Asimismo, con anterioridad al texto del EEDS, se realizó un estudio²⁷ en el que se evaluaron las normas de los Estados miembros de la UE en materia de datos sanitarios a la luz del RGPD, donde se concluyó que existía una disparidad a la hora de interpretarlo (lo que acarrea inseguridad jurídica y obstaculiza el uso secundario de los datos). Es por ello que el Reglamento EEDS se alza como una solución a esta problemática, removiendo los obstáculos para acceder a los datos sanitarios electrónicos para conseguir sus objetivos.

La promoción de la investigación y la innovación en el ámbito de la salud, facilitando la colaboración transfronteriza y el acceso a conjuntos de datos más amplios y diversos, es uno de los principales beneficios que puede ofrecer la interoperabilidad de los datos sanitarios y la implementación del Espacio Europeo de Datos Sanitarios (EEDS). Esta iniciativa no solo podría acelerar los avances médicos significativos, sino que también tendría un impacto positivo en la eficiencia del sistema de salud. Al permitir un intercambio rápido y seguro de información entre profesionales de la salud y sistemas de atención médica en toda Europa, se pueden optimizar los procesos clínicos y administrativos e incluso mejorar la gestión de los datos sanitarios y su seguridad en los sistemas. La falta de interoperabilidad de los datos sanitarios en España plantea desafíos significativos, pero el impulso hacia la creación del EEDS a nivel europeo ofrece la oportunidad de superar estas barreras y avanzar hacia una integración más efectiva y segura de los sistemas de información, teniendo en cuenta la situación ventajosa de España frente a la mayoría de los países de la Unión.

VI. FUENTES CONSULTADAS

Comisión Europea. (2019): «Estrategia Europea de datos». Disponible en: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_es

²⁷ Comisión Europea. (2021): «Evaluación de las normas de los Estados miembros de la UE sobre datos sanitarios a la luz del RGPD» (https://health.ec.europa.eu/document/download/a7f11827-f4ca-4e4d-bd7a-c15c39664010_en).

• Comisión Europea. (2021): «Evaluación de las normas de los Estados miembros de la UE sobre datos sanitarios a la luz del RGPD». Disponible en: https://health.ec.europa.eu/document/download/a7f11827-f4ca-4e4d-bd7a-c15c39664010_en

Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. (2017): Marco Europeo de Interoperabilidad – Estrategia de aplicación.

Consejo de Ministros. (2022): «El Gobierno aprueba la distribución territorial de 28 millones de euros de fondos europeos para el desarrollo de un Espacio Nacional de Datos de Salud». Nota de prensa. Ministerio de Asuntos Económicos y Transformación Digital. Disponible en: (https://portal.mineco.gob.es/RecursosNoticia/mineco/prensa/noticias/2022/20221220_ndp_distribuci%C3%B3n_inversi%C3%B3n_data_lake_sanitario.pdf).

Digital Eye Observatory (2023): «La e-pandemia. Ataques al sector sanitario». Digital Eye. Disponible en: (<https://www.digitaleye.uma.es/noticias/la-e-pandemia-ataques-al-sector-sanitario>).

Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) n°910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148.

Directiva 2011/24/UE del Parlamento Europeo y del Consejo, de 9 de marzo de 2011, relativa a la aplicación de los derechos de los pacientes en la asistencia sanitaria transfronteriza.

EIT Health (2024): «España está en condiciones de liderar en Europa la implementación del EEDS». (<https://eithealth.eu/news-article/espana-esta-en-condiciones-de-liderar-en-europa-la-implementacion-del-eeds/?lang=es>).

European Commission (2022): Commission staff working document executive summary of the impact assessment report 2022. Europa. Pág. 1.

• (2022): Commission staff working document. Impact assesment report 2022. Europa. Pág. 3.

European Data Protection Board. (2019): Directrices 1/2019 sobre códigos de conducta y organismos de supervisión con arreglo al Reglamento (UE) 2016/679.

- European Union Agency for Cybersecurity (2023): ENISA THREAT LANDSCAPE 2023. Europe. ENISA, página 13
- GARCÍA, F. J. (2023): «Introducción al espacio europeo de datos sanitarios: un nuevo horizonte en la gobernanza de datos sanitarios en la unión europea». *Actualidad Jurídica Uría Menéndez*. Página 187.
- Ley de datos. «Configurar el Futuro Digital de Europa». <https://digital-strategy.ec.europa.eu/es/policies/data-act>
- MUÑOZ, L. y GALLEGO, S. (2019): «La protección de datos y la interoperabilidad en el ámbito sanitario: dos realidades inseparables». *Derecho y Salud*, Volumen 29, Página 39.
- Portal de la Administración Electrónica. (2024): «El Espacio Nacional de Datos de Salud: un proyecto estratégico para España». Disponible en: https://administracionelectronica.gob.es/pae/Home/pae_Actualidad/pae_Noticias/2024/Abril/noticia-2024-04-19-Espacio-Nacional-Datos-Salud-proyecto-estrategico-.html
- Propuesta de Reglamento del Parlamento Europeo y del Consejo, sobre el Espacio Europeo de Datos Sanitarios.
- Propuesta de Reglamento por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial).
- Reglamento (UE) 2017/745 del Parlamento Europeo y del Consejo, de 5 de abril de 2017, sobre los productos sanitarios, y Reglamento (UE) 2017/746 del Parlamento Europeo y del Consejo, de 5 de abril de 2017, sobre los productos sanitarios para diagnóstico in vitro.
- Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) n.º 45/2001 y la Decisión n.º 1247/2002/CE.
- Reglamento (UE) 2022/868 del Parlamento Europeo y del Consejo, de 30 de mayo de 2022 relativo a la gobernanza europea de datos y por el que se modifica el Reglamento (UE) 2018/1724 (Reglamento de Gobernanza de Datos).
- Reglamento (UE) 2023/2854 del Parlamento Europeo y del Consejo, de 13 de diciembre de 2023 sobre normas armonizadas para un acceso justo a los datos y su utilización, y por el que se modifican el Reglamento (UE) 2017/2394 y la Directiva (UE) 2020/1828 (Reglamento de Datos).
- Reglamento (UE) 2024/903 del Parlamento Europeo y del Consejo, de 13 de marzo de 2024, por el que se establecen medidas a fin de garantizar un alto nivel de interoperabilidad del sector público en toda la Unión.
- Reglamento sobre la Europa Interoperable: el Consejo adopta un nuevo Reglamento para unos servicios públicos digitales más eficientes en toda la UE». <https://www.consilium.europa.eu/es/press/press-releases/2024/03/04/interoperable-europe-act-council-adopts-new-law-for-more-efficient-digital-public-services-across-the-eu/>