InDret
4.2026

Tutela jurídico-privada de los datos de salud en el Reglamento (UE) 2025/327: intimidad, autonomía y responsabilidad por daños

Luis Corpas Pastor
Universidad de Málaga

Sumario

El Reglamento (UE) 2025/327, relativo al Espacio Europeo de Datos de Salud, ordena un nuevo marco europeo de acceso, circulación e interoperabilidad de los datos de salud electrónicos. Su finalidad es doble: mejorar la asistencia sanitaria mediante el uso primario de los datos y favorecer la investigación, la innovación y la formulación de políticas públicas mediante su uso secundario. Desde el Derecho civil, sin embargo, el problema no consiste solo en determinar si el tratamiento es administrativamente lícito, sino en precisar qué tutela merece la persona cuando sus datos de salud se convierten en un recurso electrónico reutilizable, interoperable y potencialmente expuesto a brechas de seguridad, reidentificación o inferencias algorítmicas. La intimidad digital de unos datos personalísimos –como los relativos a la salud– debe ser entendida como una manifestación actual de los derechos de la personalidad y que el régimen del EEDS exige una lectura desde el derecho privado centrada en la autonomía, la diligencia reforzada, la trazabilidad y la reparación efectiva de los daños materiales y morales cuando estos acontezcan –porque la innovación regulatoria es valiosa, pero en materia de salud la eficiencia no puede convertirse en una presunción de sacrificio de los derechos de la persona–.

Abstract

Regulation (EU) 2025/327 on the European Health Data Space establishes a new European framework for access to, circulation and interoperability of electronic health data. Its purpose is twofold: to improve healthcare through the primary use of data and to promote research, innovation and public-policy making through secondary use. From the perspective of civil law, however, the central issue is not only whether the processing is administratively lawful, but also what protection must be afforded to individuals when their health data become a reusable, interoperable resource exposed to security breaches, re-identification and algorithmic inference. This article argues that digital health privacy should be understood as a contemporary expression of personality rights and that the EHDS requires a civil-law reading based on autonomy, reinforced diligence, traceability and effective compensation for material and non-material damage –because regulatory innovation is valuable, but in the realm of health, efficiency cannot become a presumption that the individual's rights are to be sacrificed–.

Title: *Private law protection of health data in EU Regulation 2025/327: privacy, autonomy and liability for damages*

Palabras clave: Espacio Europeo de Datos de Salud, datos de salud, intimidad, autonomía del paciente, responsabilidad civil, daño moral, reidentificación, ciberseguridad.
Keywords: *European Health Data Space, health data, privacy, patient autonomy, civil liability, non-material damage, re-identification, cybersecurity.*

DOI: 10.31009/InDret.2026.i4.07

InDret

4.2026

Recepción
04/06/2026
-
Aceptación
09/09/2026
-

Índice

-

1. Consideraciones preliminares
2. El dato de salud como bien jurídico civilmente protegido
2.1. Intimidad, protección de datos y derechos de la personalidad
2.2. Historia clínica, confianza y circulación digital
3. Del consentimiento informado al opt-out: autonomía sanitaria y autonomía informativa
4. Ciberseguridad, reidentificación y pérdida de control: la nueva morfología del daño
5. Responsabilidad civil por tratamiento ilícito, brecha de seguridad o reidentificación
5.1. El artículo 82 RGPD y el artículo 100 EEDS
5.2. Sujetos responsables y deberes reforzados de diligencia
5.3. Daño moral, prueba y causalidad
6. La futura Ley española de Salud Digital
7. Conclusiones y propuestas de lege ferenda
8. Bibliografía

-

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

1. Consideraciones preliminares*

El Reglamento (UE) 2025/327 del Parlamento Europeo y del Consejo, de 11 de febrero de 2025, relativo al Espacio Europeo de Datos de Salud y por el que se modifican la Directiva 2011/24/UE y el Reglamento (UE) 2024/2847 (en adelante, EEDS), constituye una de las piezas más ambiciosas del proceso europeo de construcción de espacios sectoriales de datos[1]. Su objetivo declarado es crear un marco común que facilite el acceso a los datos de salud electrónicos tanto para el uso primario, vinculado directamente a la asistencia sanitaria, como para el uso secundario, orientado a investigación, innovación, salud pública, formulación de políticas, seguridad de los pacientes o actividades de regulación. La norma no se limita a ordenar un flujo técnico de información: transforma el estatuto jurídico del dato de salud, que deja de ser solo un elemento de la historia clínica para convertirse en un activo interoperable dentro del Mercado Único Digital.

El desplazamiento del dato de salud hacia un ecosistema interoperable no crea la cuestión jurídico-privada, que ya está presente en la propia relación clínica paciente-sanitario, sino que la intensifica y le añade nuevos sujetos y riesgos. Cuando el dato sanitario se mantiene dentro de la relación clínica, el eje tradicional de protección se articula en torno a la confidencialidad, el secreto profesional, la autonomía del paciente y el consentimiento informado. Cuando el dato se desplaza a un ecosistema de reutilización, el eje se modifica: el titular ya no se relaciona solo con su médico o con el centro o profesional sanitario que lo atiende, sino con tenedores de datos, organismos de acceso, usuarios de datos, entornos seguros de tratamiento, infraestructuras transfronterizas y, eventualmente, sistemas de inteligencia artificial capaces de inferir información sensible no expresamente declarada por la persona.

El Derecho civil no puede quedar reducido, en este contexto, a una función subsidiaria posterior a la infracción administrativa. La tutela civil es la que responde a la pregunta decisiva: qué ocurre con la persona concreta cuando su intimidad sanitaria ha sido lesionada, cuando pierde el control sobre información clínica especialmente sensible, cuando sufre una brecha de seguridad, cuando es reidentificada en un conjunto aparentemente anonimizado, o cuando una inferencia algorítmica permite deducir una patología, predisposición genética o situación de vulnerabilidad. La respuesta no puede agotarse en la multa administrativa ni en la proclamación formal de derechos. La confianza en el EEDS dependerá, en nuestra opinión, de que existan remedios civiles efectivos, comprensibles y proporcionados al riesgo. El enfoque de este trabajo es, por ello, deliberadamente iuscivilista[2]. No se pretende realizar un análisis completo del Reglamento, ni explorar su dimensión administrativa, sanitaria o tecnológica. Se examina el

* Luis Corpas Pastor. (lcorpas@uma.es).

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

[2] *Cfr.* NAVAS NAVARRO (dir.), *Salud e inteligencia artificial desde el Derecho privado. Con especial atención a la pandemia por SARS-CoV-2 (covid-19),* Comares, Granada, 2021. Hasta ahora, la doctrina privatista española había abordado la protección de los datos de salud desde perspectivas sectoriales –la historia clínica, el secreto médico, la autonomía del paciente– sin enfrentarse a un marco normativo que transforme el estatuto jurídico del dato sanitario a escala europea. Esta obra colectiva singulariza la necesidad de construir respuestas desde el Derecho Civil a la digitalización sanitaria, anticipando retos que hoy el EEDS convierte en urgentes, tales como la responsabilidad por sistemas algorítmicos, la protección del dato de salud en entornos interoperables y las garantías civiles frente al pretendido uso secundario.

EEDS desde tres categorías propias del Derecho civil: la intimidad como derecho de la personalidad, la autonomía como presupuesto de legitimidad en el tratamiento de datos de salud, y la responsabilidad civil como mecanismo de reparación de daños materiales y morales. Esta perspectiva no agota el análisis del Reglamento, pero aporta un enfoque todavía no desarrollado en nuestro ámbito respecto de esta norma, publicada en marzo de 2025 y aplicable a partir de 2027.

La hipótesis central es que la interoperabilidad sanitaria solo será jurídicamente legítima si se acompaña de un sistema de tutela civil reforzada. La innovación regulatoria es valiosa, pero en materia de salud la eficiencia no puede convertirse en una presunción de sacrificio de los derechos de la persona.

Esta reflexión tiene una relevancia particular para España. El Ministerio de Sanidad ha iniciado el proceso de elaboración de una futura Ley de Salud Digital para adaptar el ordenamiento nacional al EEDS, extender la historia clínica digital interoperable, regular el uso de tecnologías emergentes y organizar la gobernanza del uso primario y secundario de datos de salud[3]. En un sistema sanitario descentralizado, en el que las comunidades autónomas ostentan competencias esenciales de gestión sanitaria, el problema no será únicamente técnico. Será también jurídico-civil: cómo asegurar que la persona reciba una protección homogénea, que pueda ejercer de forma real sus derechos y que disponga de vías eficaces de reparación cuando la digitalización sanitaria cause daños. Por este motivo, la consulta pública previa sobre la futura Ley española de Salud Digital, publicada por el Ministerio de Sanidad en septiembre de 2025, convierte el presente estudio en una aportación de oportunidad singular para el debate legislativo nacional. La norma proyectada deberá adaptar el ordenamiento interno al EEDS y desarrollar aquellas previsiones organizativas, técnicas, procedimentales y sancionadoras que el propio Reglamento remite al Derecho nacional, en un sistema sanitario descentralizad en el que las comunidades autónomas gestionan servicios de información con distintos grados de madurez tecnológica e institucional[4].

Adicionalmente, la reflexión civil resulta necesaria porque el EEDS opera sobre una tensión que atraviesa todo el Derecho privado contemporáneo: la tensión entre utilidad colectiva de los datos y protección de la persona concreta. La salud pública, la investigación biomédica y la innovación tecnológica justifican un uso intenso de datos, pero no autorizan a tratar al paciente como una mera fuente de información. A nuestro juicio, la persona no desaparece detrás del dato, al contrario, el dato de salud conserva una dimensión biográfica y relacional que obliga a repensar las categorías clásicas de intimidad, consentimiento, diligencia y daño. Conviene detenerse en una cuestión que la doctrina civilista ha comenzado a afrontar con creciente rigor: la de si el dato de salud puede ser objeto de relaciones patrimoniales sin perder su naturaleza personalísima. La pregunta no es retórica. El considerando 2 del Reglamento (UE) 2022/868 sobre gobernanza de

[3] Ministerio de Sanidad, consulta pública previa sobre el futuro Proyecto de Ley de Salud Digital, 22 septiembre 2025. La nota ministerial identifica como objetivos la adaptación al Reglamento (UE) 2025/327, la interoperabilidad de la historia clínica, la regulación de tecnologías digitales y el tratamiento de datos personales de salud en el Sistema Nacional de Salud con fines de interés público. https://www.sanidad.gob.es/gl/gabinete/notasPrensa.do?id=6750.

[4] La doctrina civil española ha comenzado a abordar la protección de los datos de salud en entornos digitales, pero todavía no ha desarrollado de forma suficiente qué previsiones específicas de Derecho privado debería incorporar la futura Ley de Salud Digital para garantizar la efectividad de los remedios civiles en caso de brecha de seguridad, reidentificación o inferencia algorítmica sobre datos de salud.

datos ya reconoce que los datos pueden ser un recurso valioso y que su reutilización genera valor económico. El EEDS prolonga esa lógica al sector sanitario. Sin embargo, la admisión de un valor económico del dato no equivale a su plena patrimonialización.

Como ha señalado ZECH, el dato digital no encaja cómodamente en las categorías tradicionales del derecho de propiedad, porque no es rival –puede usarse simultáneamente por varios sujetos sin exclusión– ni agotable[5]. Esta inespecificidad obliga al Derecho civil a construir una categoría intermedia: la del dato como bien de interés personal cuya explotación económica es posible pero no incondicionada.

En materia sanitaria, esa condición se intensifica. La reutilización comercial de datos de salud –aunque sea indirecta, mediada por la investigación aplicada o por desarrollos de inteligencia artificial– no puede eludir la consideración de que el origen del dato reside en una persona concreta que confió información íntima en un contexto terapéutico, dando por hecho que el profesional no traicionaría dicha confianza.

La ausencia de una contraprestación directa al paciente, y la opacidad sobre los beneficios derivados del uso secundario, plantean un problema de justicia distributiva que el Derecho civil no puede ignorar indefinidamente. En este sentido, la categoría del enriquecimiento injusto podría ofrecer, en determinados supuestos de explotación comercial masiva de datos de salud sin adecuada compensación o transparencia, un cauce civil complementario a la responsabilidad por daños, en un proceso similar al cambio que se produjo sobre el carácter autónomo del daño a la autonomía decisoria del paciente cuando existe ausencia de información o inexistencia de un consentimiento informado válido[6].

Una última precisión metodológica resulta necesaria. A lo largo de este trabajo se distingue entre el análisis del Derecho vigente (de lege lata) y las propuestas dirigidas al legislador (de lege ferenda). Cuando se emplean expresiones como «a nuestro juicio» o «en nuestra opinión» para introducir una interpretación de normas o principios ya vigentes, se está formulando una lectura del Derecho actual, sujeta como toda interpretación doctrinal a discusión; pero no una propuesta de reforma. Cuando, en cambio, se utiliza la fórmula «de lege ferenda» o se afirma que algo «debería» ser reconocido, regulado o presumido, se está formulando una propuesta para la futura Ley española de Salud Digital u otra norma de desarrollo, no una descripción del Derecho hoy vigente. Se ha procurado mantener esta distinción de forma expresa en los pasajes en que ambas perspectivas podrían confundirse, particularmente en materia de responsabilidad civil.

[5] ZECH, «A legal framework for a data economy in the European Digital Single Market: rights in data», Journal of *Intellectual Property Law & Practice*, vol. 11, núm. 6, 2016, pp. 460-470. DOI: https://doi.org/10.1093/jiplp/jpw072.

[6] *Vid.* EVANGELIO LLORCA, «Responsabilidad civil e inteligencia artificial en el ámbito sanitario», en ÁLVAREZ LATA, (coord.) *et al., Derecho de contratos, responsabilidad extracontractual e inteligencia artificial*, Aranzadi, Cizur Menor, 2024, pp. 149-222. La doctrina científica ha consolidado la autonomía del paciente como eje del régimen de responsabilidad médica. La infracción del deber de información y la ausencia de consentimiento informado válido constituyen actualmente títulos autónomos de imputación, con independencia del resultado asistencial, conforme a una jurisprudencia bien asentada del Tribunal Supremo. Sin embargo, la traslación de ese principio de autonomía al entorno del uso secundario de datos de salud no ha sido objeto de estudio específico en la literatura española posterior al EEDS. El modelo de *opt-out* del artículo 71 del Reglamento introduce una quiebra relevante con la tradición del consentimiento informado en su modalidad activa: el silencio del paciente pasa a operar, por defecto, en favor de la disponibilidad del dato para fines de investigación, innovación o políticas públicas.

2. El dato de salud como bien jurídico civilmente protegido

Los datos de salud pertenecen al núcleo más sensible de la información personal. No revelan solo un episodio clínico aislado, pueden expresar la biografía corporal de una persona, su vulnerabilidad, sus hábitos, su exposición a riesgos, su herencia genética, sus relaciones familiares o incluso su expectativa vital. Por ello, el dato sanitario no puede analizarse como una mera unidad informacional.

Desde el Derecho civil, se integra en la esfera de los derechos de la personalidad y conecta directamente con la intimidad, la dignidad y la autodeterminación. En esta línea, los derechos de la personalidad han de ser interpretados dinámicamente, atendiendo a las condiciones sociales y tecnológicas en que se ejercen[7]. En el plano de los datos personales, Rebollo Delgado ha descrito la evolución del derecho fundamental a la protección de datos como respuesta progresiva a la expansión tecnológica, insistiendo en la necesidad de dotar al ciudadano de poderes efectivos de control frente al tratamiento de su información[8]. La novedad que aporta el presente trabajo es la articulación de esa lectura de los derechos de la personalidad con el dato de salud en el marco específico del EEDS: un dato que, por su naturaleza biográfica y relacional –y, en determinados supuestos, como los datos genéticos, genómicos o los derivados de dispositivos de identificación fisiológica, también biométrica–, no puede ser tratado simplemente como información patrimonializable sin perder su dimensión personalísima. La categoría intermedia que aquí se propone –dato de salud como bien de interés personal cuya explotación económica es posible pero no incondicionada– no aparece todavía consolidada en esos términos en la doctrina española y constituye una de las contribuciones teóricas centrales de este trabajo.

La Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, parte de esta premisa cuando reconoce que toda persona tiene derecho a que se respete el carácter confidencial de los datos referentes a su salud y a que nadie pueda acceder a ellos sin previa autorización amparada por la ley[9]. La confidencialidad no es una mera regla burocrática: es la traducción jurídica de una relación de confianza con el profesional sanitario. El paciente revela datos que, fuera de la relación asistencial, probablemente no compartiría. Esa revelación se justifica por la finalidad terapéutica y queda rodeada de deberes de secreto, custodia y uso limitado de tales datos.

El EEDS altera parcialmente esta arquitectura al impulsar la interoperabilidad y la reutilización. La alteración no es necesariamente ilegítima, pero sí exige una reconstrucción de las garantías. El artículo 1 del Reglamento establece reglas, normas e infraestructuras comunes para facilitar

[7] García Rubio, «Los derechos de la personalidad», en Gete-Alonso y Calera/Solé Resina (coords.), *Tratado de Derecho de la persona física*, Civitas-Thomson Reuters, Cizur Menor, 2013, pp. 595-631.

[8] Rebollo Delgado, El derecho fundamental a la protección de datos personales, Dykinson, Madrid, 2018.

[9] Artículo 7.1 de la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica. Sobre la conexión entre historia clínica, confidencialidad y acceso indebido, CASANOVA ASENCIO, «Protección de datos en el ámbito de la historia clínica: el acceso indebido por el personal sanitario y sus consecuencias», *InDret*, núm. 2, 2019, p. 26.

el acceso a datos de salud electrónicos a efectos de uso primario y secundario[10]. El dato de salud pasa así de un modelo relacional, centrado en la historia clínica y en el prestador sanitario, a un modelo ecosistémico, donde distintas entidades pueden intervenir en la puesta a disposición, autorización, acceso, tratamiento y supervisión.

Por consiguiente, la pregunta desde el derecho civil no es solo si existe base jurídica para el tratamiento, sino qué posición conserva el titular de los datos de salud frente a esa circulación ampliada. Por otra parte, la eventual licitud administrativa del tratamiento no agota la legitimidad civil de la injerencia. En nuestra opinión, un sistema jurídicamente correcto debe permitir al ciudadano conocer, controlar y, en su caso, reclamar por el uso de sus datos, especialmente cuando estos reflejan aspectos íntimos de su identidad sanitaria.

2.1. Intimidad, protección de datos y derechos de la personalidad

El Derecho civil debe interpretar esta evolución a la luz de los derechos de la personalidad. La intimidad no se agota en el secreto de lo ya oculto. En la sociedad digital, la lesión puede producirse también por agregación, correlación o inferencia. Un dato aislado puede parecer neutro, pero su cruce con otros datos puede revelar información íntima. Una historia clínica desidentificada puede volverse identificable si se combina con información genómica, localización, edad, enfermedad rara o datos disponibles en fuentes externas. La protección civil debe atender, por tanto, no solo al acceso ilícito clásico, sino a la pérdida de control sobre el contexto de uso.

La doctrina constitucional española refuerza esta lectura. El Tribunal Constitucional ha distinguido el derecho a la intimidad del derecho fundamental a la protección de datos, señalando que este último atribuye a la persona un poder de control sobre sus datos personales, sobre su uso y destino, para impedir un tráfico ilícito o lesivo para la dignidad del afectado[11]. En materia sanitaria, esta distinción tiene especial importancia. Puede existir una lesión de la protección de datos aunque el contenido no haya sido difundido públicamente, basta con que la persona pierda el control jurídico sobre un dato cuyo tratamiento excede la finalidad, base legal o garantía exigible.

Esta separación entre intimidad y protección de datos resulta decisiva para el dato sanitario. La lesión no se produce solo cuando la información se difunde públicamente, sino también cuando se rompe el poder de disposición jurídica sobre su circulación, uso o destino. En este sentido, la protección de datos opera como una garantía autónoma de control frente a infraestructuras que tratan información personal a gran escala[12]. Esta construcción resulta más sólida si se parte de una categoría unitaria de los derechos fundamentales de la personalidad. Honor, intimidad, propia imagen y protección de datos no operan como compartimentos cerrados cuando la lesión procede de la circulación digital de información personal, se proyectan sobre un mismo centro

[10] Reglamento (UE) 2025/327 del Parlamento Europeo y del Consejo, de 11 de febrero de 2025, relativo al Espacio Europeo de Datos de Salud y por el que se modifican la Directiva 2011/24/UE y el Reglamento (UE) 2024/2847, art. 1.1.

[11] STC 292/2000, de 30 de noviembre, FFJJ 5 y 6. Vid. también STC 58/2018, de 4 de junio, especialmente sobre la dimensión específica del artículo 18.4 CE.

[12] González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU,* Springer, Cham, 2014.

de gravedad, que es el señorío jurídico de la persona sobre los atributos esenciales de su identidad. Por eso, en materia sanitaria, la autodeterminación informativa no debe entenderse como un derecho meramente procedimental, sino como una manifestación civil de la personalidad frente a tratamientos capaces de recomponer, clasificar o exponer la vida íntima del paciente[13].

De igual manera, la fuerza expansiva de los derechos fundamentales obliga a leer cualquier regulación civil o administrativa desde el prisma constitucional. Prieto Sanchís ha señalado que los derechos fundamentales irradian sobre el conjunto del sistema, hasta el punto de que detrás de cada precepto legal puede advertirse una norma constitucional que lo confirma o contradice14. Esta idea resulta especialmente útil en el EEDS: detrás de cada regla de interoperabilidad, de cada permiso administrativo y de cada entorno seguro se encuentra la pregunta por el respeto a la dignidad, la intimidad y la autodeterminación informativa.

Asimismo, la protección de datos personales no puede entenderse ya como un mecanismo puramente instrumental. Rebollo Delgado describe su evolución como una respuesta progresiva a la expansión tecnológica y a la necesidad de dotar al ciudadano de poderes frente al tratamiento de su información personal[15]. Sumado a esto, en la era digital la tutela civil de los datos sanitarios debe enlazar con una idea material de control: no basta con que el dato no se publique, es necesario que el titular pueda saber qué se hace con él, por quién, con qué finalidad y bajo qué responsabilidad[16].

Por ello, el dato de salud debe ser tratado como un bien jurídico civilmente protegido, aunque no sea un bien patrimonial en sentido estricto. La información sanitaria pertenece a la esfera personalísima, pero puede circular, ser explotada, generar valor y producir daños. Esta doble naturaleza -personalísima y económicamente útil- explica buena parte de los problemas del EEDS. El riesgo civil aparece cuando la utilidad colectiva del dato de salud electrónico desplaza la consideración de la persona que originó el dato de salud.

A esta exigencia debe añadirse una dimensión estructural de la transparencia. En un ecosistema de reutilización masiva, la persona afectada difícilmente podrá controlar sus datos si los conjuntos utilizados no están descritos de forma homogénea, actualizada y comprensible. La identificación de la fuente, el alcance, las categorías de datos, las variables incluidas, la procedencia, la cobertura temporal y las condiciones de disponibilidad no constituye una cuestión meramente técnica. Desde el Derecho civil, cumple una función de garantía: permite reconstruir el itinerario del dato, valorar si el uso se mantuvo dentro de la finalidad autorizada y

[13] De Verda y Beamonte, «Los derechos fundamentales de la personalidad (al honor, a la intimidad y a la propia imagen) como categoría unitaria», *Revista Boliviana de Derecho*, núm. 23, 2017, pp. 54-111; Caballero Trenado, «Cartografía legal de la autodeterminación informativa digital. Un derecho de construcción jurisprudencial», *Universitas*, núm. 35, 2021, pp. 2-27.

[14] Prieto Sanchís, «El constitucionalismo de los derechos», *Revista Española de Derecho Constitucional*, vol. 24, núm. 71, 2004, p. 51.

[15] Rebollo Delgado, 2018, cit., pp. 68-71.

[16] *Cfr.* Rubí Puig, «Daños por infracciones del derecho a la protección de datos personales. El remedio indemnizatorio del artículo 82 RGPD», *Revista de Derecho Civil*, vol. V, núm. 4, 2018, pp. 62-73. En el ámbito del RGPD, la legitimación pasiva de los «sujetos responsables» se ha estudiado convenientemente. Sin embargo, conviene señalar la existencia de nuevos «responsables» en los daños a los que se refiere el art. 100 del Reglamento (UE) 2025/327 porque, sobre todo, los conceptos de tratamiento de datos y usos secundarios no tienen plena identidad de razón.

determinar, en su caso, quién debe responder por una brecha, una reidentificación o un tratamiento desviado[17].

2.2. Historia clínica, confianza y circulación digital

La historia clínica ha sido tradicionalmente el espacio documental de la relación asistencial. En ella confluyen datos objetivos, apreciaciones profesionales, antecedentes, pruebas, diagnósticos y decisiones terapéuticas. Su régimen jurídico no puede separarse de la confianza que permite al paciente revelar información íntima. Ordás Alonso ha destacado la conexión entre intimidad, secreto médico y protección de datos sanitarios al analizar la historia clínica como ámbito especialmente sensible de reserva[18]. De la misma manera, la Ley 41/2002 separa el uso asistencial de la historia clínica de otros accesos, precisamente porque el dato fue entregado en un marco funcional y fiduciario.

El EEDS no destruye ese marco, pero lo desplaza. El uso primario mantiene una conexión directa con la asistencia sanitaria. En cambio, el uso secundario se separa de la relación clínica inmediata y permite que el dato sirva a finalidades de investigación, innovación, salud pública o formulación de políticas. A nuestro juicio, esta separación impone una exigencia adicional de transparencia: el paciente debe poder comprender que el dato que entregó para ser curado puede circular después en un ecosistema institucional distinto.

Igualmente, la digitalización sanitaria introduce una dimensión territorial y transfronteriza que altera la relación clásica entre paciente y prestador. La historia clínica interoperable permite continuidad asistencial y puede evitar errores médicos, duplicidades y retrasos. Sin embargo, también multiplica los puntos de acceso y los posibles fallos de custodia. La confianza deja de depender solo del médico o del hospital y pasa a depender de una arquitectura completa de seguridad, registro, trazabilidad y responsabilidad.

Por lo tanto, desde una perspectiva civil, la historia clínica digital interoperable debe ser vista como una institución de confianza reforzada. Su legitimidad no deriva solo de su eficiencia, sino de la capacidad del sistema para preservar la confidencialidad, limitar los accesos, registrar las operaciones y reparar de forma efectiva los daños. En materia sanitaria, la confianza no es un elemento psicológico accesorio: es una condición de funcionamiento del sistema.

Esta consideración de la historia clínica digital como institución de confianza permite sugerir una categoría conceptual que la doctrina civil todavía no ha desarrollado con suficiente detalle en el contexto del EEDS: la de la obligación de lealtad del tenedor de datos sanitarios frente al paciente. En la tradición angloamericana, la relación fiduciaria genera deberes de lealtad que van más allá de la mera diligencia: quien ostenta una posición de confianza no puede usar la información del beneficiario en su propio interés ni en interés de terceros sin autorización

[17] De Miguel Beriain/López De La Peña De Pablo/Loyo-Menoyo, «El nuevo reglamento europeo relativo al espacio europeo de datos de salud: su impacto en la gobernanza del dato y su uso ético y seguro», Revista de Derecho y Genoma Humano, núm. 61, 2025, pp. 1-30; Loza Corera, «Datos y gobernanza de datos y conexiones con principios protección de datos en el artículo 10 del Reglamento», en Cotino Hueso/Simón Castellano (dirs.), *Tratado sobre el Reglamento de Inteligencia Artificial de la Unión Europea*, 2024, pp. 565-591.

[18] Ordás Alonso, «Intimidad, secreto médico y protección de datos sanitarios», en García Amado (coord.), *Razonar sobre derechos*, Tirant lo Blanch, Valencia, 2016, pp. 779-783.

expresa. La relación médico-paciente ha sido identificada, desde Pellegrino, como paradigma de relación fiduciaria en el ámbito sanitario[19]. Si esa dimensión fiduciaria se traslada a los tenedores de datos del EEDS, la consecuencia es que estos no solo están obligados a no revelar sin autorización, sino que están positivamente impedidos de explotar la información más allá de la finalidad consentida, aunque esa explotación no sea detectada ni genere un daño inmediato. En nuestro Ordenamiento, la obligación de buena fe del artículo 7 del Código Civil y los deberes de información y lealtad en las relaciones de confianza ofrecen anclajes dogmáticos para esta construcción[20]. A nuestro juicio, la figura del tenedor de datos del artículo 2.18 del EEDS –que gestiona datos de salud sin ser necesariamente el prestador sanitario– no puede quedar definida solo por sus obligaciones técnicas y administrativas. Su posición jurídica debe ser construida, desde el Derecho civil, como la de un sujeto que ostenta un encargo de confianza sobre información ajena, con los consiguientes deberes de no auto beneficiarse, de actuar en interés del titular y de rendir cuentas de toda operación de tratamiento. Se trata, en todo caso, de una propuesta de lectura del Derecho vigente –no de un enunciado normativo ya consolidado por la jurisprudencia–, cuya plena eficacia práctica dependería de que la futura Ley española de Salud Digital la recogiera expresamente. Con esa salvedad, esta reconstrucción podría derivarse de los principios generales del Derecho civil y de la aplicación sistemática del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, General de Protección de Datos (en adelante, RGPD) y el EEDS interpretados a la luz del artículo 10 CE.

El uso primario confirma esta lectura. Los derechos de acceso, portabilidad, introducción de información en la historia clínica, conocimiento de accesos y limitación frente a determinados profesionales no son meras facultades administrativas añadidas al sistema. Desde una perspectiva civil, son manifestaciones concretas del control personal sobre la propia biografía sanitaria y permiten que la interoperabilidad asistencial no se construya a costa de convertir al paciente en un sujeto pasivo del flujo informacional[21].

El derecho de acceso a la historia clínica confirma, además, que el control del paciente no puede confundirse con una apertura indiscriminada de información. La historia clínica contiene datos objetivos, valoraciones profesionales, anotaciones subjetivas, información de terceros y, en ocasiones, datos relativos a personas fallecidas o a familiares. De ahí que el acceso deba ser efectivo, pero jurídicamente ordenado: debe permitir al paciente conocer la información relevante para su salud y para la defensa de sus derechos, sin desconocer los límites derivados de la intimidad de terceros, de las anotaciones subjetivas legítimamente reservables y de la confidencialidad profesional. En el entorno digital, esta misma lógica exige un derecho operativo a conocer los accesos producidos, porque sin registro de accesos no hay control real, y sin control real la autonomía informativa se convierte en una declaración puramente retórica[22].

---

[19] PELLEGRINO y THOMASMA, *A Philosophical Basis of Medical Practice*, Oxford University Press, New York, 1981, pp. 159-180.

[20] DÍEZ-PICAZO, *La doctrina de los propios actos*, Bosch, Barcelona, 1963, pp. 189-220. Para el marco actual del art. 7 CC: DÍEZ-PICAZO/GULLÓN BALLESTEROS, *Sistema de Derecho Civil*, vol. I, 12.ª ed., Tecnos, Madrid, 2012, pp. 420-435.

[21] DE MIGUEL BERIAIN, «Los derechos relativos al uso primario de los datos personales en el Reglamento del Espacio Europeo de Datos de Salud. Una visión panorámica», *Revista Jurídica de Castilla y León*, núm. 64, 2025, pp. 71-96; JORQUI AZOFRA, «Derechos y disposiciones relativas al uso primario de los datos de salud electrónicos personales», en EGUSQUIZA BALMASEDA/LUQUIN BERGARECHE/JORQUI AZOFRA/VIDÁN PEÑA, *Régimen jurídico de protección de datos de salud en el Espacio Europeo de Datos de Salud (EEDS),* 2025, pp. 49-114.

[22] SAIZ RAMOS/LARIOS RISCO, «El derecho de acceso a la historia clínica por el paciente: propuesta para la reserva de anotaciones subjetivas», *Derecho y Salud*, vol. 18, núm. 1, 2009, pp. 21-41; LOPEZ ULLA, «El acceso a los datos

3. Del consentimiento informado al opt-out: autonomía sanitaria y autonomía informativa

La autonomía de la voluntad es uno de los pilares del Derecho civil. En el ámbito sanitario adopta una forma específica: la autonomía del paciente. La Ley 41/2002 reconoce que toda actuación en el ámbito de la salud requiere, con carácter general, el consentimiento libre y voluntario del afectado una vez recibida la información adecuada[23]. El consentimiento informado no se limita a autorizar un acto médico, expresa una concepción de la persona como sujeto capaz de decidir sobre su cuerpo, su salud y su información.

El EEDS introduce un cambio relevante. En el uso primario, el Reglamento complementa derechos de acceso, portabilidad, rectificación y control sobre los datos electrónicos de salud. En el uso secundario, sin embargo, la lógica se aproxima a un modelo de habilitación legal, autorización institucional y derecho de autoexclusión. El artículo 71 reconoce el derecho de las personas físicas a optar por que sus datos de salud electrónicos no sean tratados para uso secundario, pero configura ese derecho como salida de un sistema que parte de la disponibilidad inicial del dato[24].

Conviene no simplificar el problema. El Reglamento General de Protección de Datos (en adelante, RGPD) no es un régimen construido exclusivamente sobre el consentimiento. Para categorías especiales de datos, como los datos de salud, el artículo 9 RGPD establece una prohibición general de tratamiento salvo que concurra alguna de las excepciones previstas, entre ellas el consentimiento explícito, la asistencia sanitaria, la salud pública o la investigación científica con garantías adecuadas[25]. Por consiguiente, el problema no es que el EEDS sustituya siempre consentimiento por poder público, sino que para el uso secundario desplaza el centro de gravedad desde la voluntad individual hacia la autorización institucional.

A nuestro juicio, debe distinguirse entre consentimiento como base jurídica del tratamiento y consentimiento como expresión de autonomía. El primero pertenece a la técnica del RGPD, el segundo pertenece al estatuto civil de la persona. Que un tratamiento sea lícito por una base legal distinta del consentimiento no significa necesariamente que la autonomía resulte irrelevante. El *opt-out* del artículo 71 EEDS conserva una forma de elección, pero es una elección reactiva: el ciudadano debe oponerse para salir de un circuito que, por defecto, puede estar orientado a la reutilización.

relativos a la salud: criterios aplicables de acuerdo con la Ley de transparencia y a la luz de la jurisprudencia del Tribunal Europeo de Derechos Humanos», *Papeles el tiempo de los derechos*, núm. 12, 2018, pp. 1-21; BELTRAN AGUIRRE, «Tratamiento de datos de salud en la prestación de servicios sociales», Derecho y Salud, vol. 18, núm. 1, 2009, pp. 1-19; CASANOVA ASENCIO, «Protección de datos en el ámbito de la historia clínica: el acceso indebido por el personal sanitario y sus consecuencias», *InDret*, núm. 2, 2019, pp. 1-31.

[23] Artículos 8 y 10 de la Ley 41/2002. Sobre el Convenio de Oviedo como refuerzo de la autonomía del paciente, DE MIGUEL BERIAIN/LAZCOZ MORATINOS, «El Convenio de Oviedo, veinte años después de su firma. Algunas sugerencias de enmienda», *Quaestio Iuris*, vol. 11, núm. 1, 2018, p. 448.

[24] Reglamento (UE) 2025/327 del Parlamento Europeo y del Consejo, de 11 de febrero de 2025, relativo al Espacio Europeo de Datos de Salud y por el que se modifican la Directiva 2011/24/UE y el Reglamento (UE) 2024/2847, art. 71.

[25] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, General de Protección de Datos (en adelante, RGPD), arts. 6, 9 y 89.

De igual manera, el *opt-out* solo será jurídicamente valioso si es real, inteligible y ejercitable. La autoexclusión formal, escondida en portales digitales complejos o redactada en términos incomprensibles, no satisface la exigencia civil de autonomía. La persona debe recibir información clara sobre qué datos se reutilizan, para qué finalidades, por qué sujetos, durante cuánto tiempo y con qué consecuencias. Además, debe poder revocar su decisión y ejercerla sin cargas desproporcionadas.

La información previa al ejercicio del *opt-out* debe responder a un estándar material, no meramente formal. La reciente doctrina del Tribunal Supremo sobre transparencia algorítmica de la Administración –dictada en un contexto distinto, pero trasladable por analogía a la exigencia de información material que aquí se defiende– exige, frente a decisiones o sistemas automatizados que condicionan derechos o prestaciones de los ciudadanos, un conocimiento efectivo de su funcionamiento y no una mera explicación formularia[26]. En la tradición del consentimiento informado, la validez de la decisión depende de que el paciente conozca los riesgos, alternativas y consecuencias relevantes para decidir. Trasladado al uso secundario de datos, ello implica que la persona debe comprender qué categorías de datos se reutilizan, para qué finalidades, con qué garantías, qué sujetos pueden acceder y qué riesgos razonables existen de inferencia, reidentificación o uso algorítmico. Esta exigencia se intensifica respecto de menores y personas vulnerables, pues la prestación del consentimiento o el ejercicio de la autoexclusión no pueden separarse de la protección de la intimidad familiar, del interés superior del menor y de su progresiva capacidad de decisión[27].

El artículo 71 EEDS exige que el derecho pueda ejercerse en cualquier momento, sin necesidad de motivación y de forma reversible, también exige que el mecanismo sea accesible y fácilmente comprensible[28]. Sin embargo, el Reglamento deja a los Estados miembros un margen relevante en la concreción del mecanismo. Por ello, la futura legislación española debería evitar que el derecho se convierta en una garantía desigual según comunidad autónoma, prestador sanitario o nivel de alfabetización digital.

Asimismo, la opción por un modelo de autoexclusión debe interpretarse a la luz del artículo 9.4 RGPD, que permite a los Estados miembros mantener o introducir condiciones adicionales, incluso limitaciones, para el tratamiento de datos genéticos, biométricos o relativos a la salud[29]. El EEDS intenta reducir esa fragmentación, pero no la elimina por completo. En nuestra opinión,

[26] *Vid.* STS 1119/2025, Contencioso-administrativo, de 11 de septiembre de 2025 (ECLI:ES:TS:2025:3826) (caso Civio/BOSCO, FD noveno).

[27] CADENAS OSUNA, «El estándar de información sanitaria sobre riesgos de los tratamientos e intervenciones médicas en España y el common law: una visión panorámica», *InDret,* núm. 4, 2016, pp. 1-42; VILLANUEVA TURNES, «El derecho a la intimidad y el consentimiento de los menores de edad. Especial referencia a las redes sociales», *Revista Boliviana de Derecho*, núm. 23, 2017, pp. 208-221; SÁNCHEZ GÓMEZ, «Las nuevas tecnologías y su impacto en los derechos al honor, intimidad, imagen y protección de datos del menor. Mecanismos jurídicos de protección: carencias, interrogantes y retos del legislador», *Revista Boliviana de Derecho*, núm. 23, 2017, pp. 168-191; RECUERO, «El uso secundario de datos de salud electrónicos: el futuro Reglamento del Espacio Europeo de Datos de Salud y su interacción con la protección de datos personales», *InDret*, núm. 2, 2024, pp. 525-551.

[28] Reglamento (UE) 2025/327, art. 71. Este precepto establece el derecho de autoexclusión respecto del uso secundario, su reversibilidad, la necesidad de mecanismos accesibles y comprensibles, el efecto sobre permisos posteriores y las condiciones de eventuales excepciones nacionales.

[29] RGPD, art. 9.4. Sobre la fragmentación derivada de la facultad de especificación nacional, *vid.* Comisión Europea, *Proposal for a Regulation on the European Health Data Space*, COM(2022) 197 final, 3 mayo 2022, *Impact Assessment*, apart. 3.2.

la tensión entre armonización europea y diversidad nacional se proyectará especialmente sobre la forma de informar, registrar y hacer oponible el *opt-out*.

También debe advertirse que la autonomía informativa no se agota en decir sí o no. Puede requerir niveles de granularidad: no es lo mismo permitir el uso de datos para investigación pública en enfermedades raras que permitir su empleo por entidades privadas en desarrollos comerciales de inteligencia artificial. El Reglamento establece finalidades permitidas y prohibidas, pero la percepción civil del riesgo puede variar según finalidad, sujeto y sensibilidad del dato. Del mismo modo, el ciudadano puede aceptar una reutilización solidaria y rechazar una reutilización económicamente orientada.

Desde la perspectiva del Derecho civil de la persona, la cuestión de la granularidad del consentimiento no es un tecnicismo regulatorio sino una exigencia de coherencia con el principio de autonomía. La Ley 41/2002 consagró la autonomía del paciente como principio rector de la relación asistencial, el RGPD extendió esa autonomía al plano informativo, y el EEDS debe completar esa proyección en el ámbito del uso secundario. Ahora bien, la autonomía informativa no funciona en el vacío: requiere información suficiente, capacidad real de comprensión y ausencia de presiones contextuales que desvirtúen la decisión. En este punto, la doctrina anglosajona de la *contextual integrity,* desarrollada por NISSENBAUM, resulta especialmente iluminadora: la legitimidad del flujo informativo no depende solo de que el sujeto haya consentido, sino de que la información circule en un contexto normativo congruente con aquel en que fue originalmente revelada[30]. Trasladada al EEDS, esta idea implica que el dato entregado en la consulta médica no fluye legítimamente hacia un sistema de inteligencia artificial comercial con el solo respaldo de una base legal administrativa, aunque esta sea formalmente válida. El Derecho civil debe exigir que la arquitectura del *opt-out* sea congruente con esa expectativa contextual razonable del paciente. Ello supone, entre otras consecuencias, que la ausencia de respuesta activa del ciudadano no puede interpretarse sin más como manifestación de voluntad favorable al uso secundario: el silencio informativo no equivale al consentimiento tácito, máxime cuando la complejidad del ecosistema impide a la mayoría de ciudadanos comprender las implicaciones reales de su omisión.

Por consiguiente, la futura Ley española de Salud Digital debería configurar el opt-out como un derecho de ejercicio sencillo, multicanal, reversible, documentado y portable. Debe poder ejercerse digitalmente, pero también por vías no digitales. Debe ser comprensible para personas mayores, personas con discapacidad y ciudadanos sin habilidades tecnológicas. Y, además, debe proyectarse sobre prestadores públicos y privados, porque la intimidad sanitaria no puede depender del circuito asistencial al que pertenezca la historia clínica.

La autonomía informativa también debe proyectarse sobre la intervención de sistemas de inteligencia artificial en la asistencia sanitaria. Cuando una herramienta algorítmica influya de modo significativo en el diagnóstico, la priorización o el tratamiento, no basta con que exista formalmente un profesional en el circuito. La intervención humana debe ser material, competente y capaz de modificar la recomendación automatizada, además, el paciente debe

[30] NISSENBAUM, Privacy in Context: Technology, Policy, and the Integrity of Social Life, Stanford University Press, Stanford, 2010, pp. 127-157.

conservar un margen real para conocer esa intervención y, en los términos compatibles con la buena práctica clínica, oponerse a que la decisión quede absorbida por el sistema técnico[31].

4. Ciberseguridad, reidentificación y pérdida de control: la nueva morfología del daño

La ciberseguridad sanitaria ya no puede considerarse una cuestión meramente técnica. Desde el Derecho civil, integra el contenido de los deberes de diligencia y custodia. Quien conserva, permite acceder o facilita el uso de datos de salud asume una obligación reforzada de seguridad, porque el daño previsible no consiste solo en la pérdida de disponibilidad de un sistema, sino en la exposición de información íntima. Casarosa ha mostrado que el sector sanitario presenta riesgos específicos en la intersección entre dispositivos conectados, ciberseguridad y protección jurídica de datos[32].

Si el dato sanitario es especialmente sensible, la obligación de custodia debe ser igualmente reforzada. La brecha de seguridad no produce únicamente una incidencia informática: puede desencadenar una intromisión en la intimidad, una pérdida de control sobre datos personales, un riesgo de discriminación y un daño moral autónomo. Sumado a esto, la naturaleza digital del dato permite que la lesión se replique, se conserve y se proyecte en el tiempo de forma difícilmente reversible.

El Reglamento reconoce la importancia de la anonimización, la seudonimización y los entornos seguros de tratamiento. Para el uso secundario, los datos personales deben ponerse a disposición preferentemente en formato anonimizado y, cuando resulte necesario el tratamiento de datos personales, en formato seudonimizado[33]. Además, el acceso debe realizarse en entornos seguros sometidos a condiciones técnicas y organizativas estrictas. Estas garantías son necesarias, pero no eliminan el riesgo. La anonimización absoluta es especialmente problemática en datos genómicos, enfermedades raras o conjuntos de datos de gran granularidad.

La diferencia entre dato anónimo y dato seudonimizado es decisiva. El dato anonimizado queda fuera del RGPD cuando la identificación ya no es razonablemente posible. El dato seudonimizado, en cambio, sigue siendo dato personal porque la reidentificación permanece posible mediante información adicional. En salud, la frontera entre ambas categorías es particularmente inestable. La singularidad clínica, la combinación de variables y la disponibilidad de fuentes externas pueden convertir en identificable un conjunto que parecía neutralizado.

La experiencia de los biobancos y de la investigación biomédica confirma esta cautela. La seudonimización constituye una medida útil para equilibrar investigación y derechos de la

[31] DE MIGUEL BERIAIN, «Should we have a right to refuse diagnostics and treatment planning by artificial intelligence?», Medicine, *Health Care and Philosophy*, vol. 23, 2020, pp. 247-252. *Vid.* DE MIGUEL BERIAIN/SANZ/LAZCOZ MORATINOS, «Machine learning in the EU health care context: exploring the ethical, legal and social issues», *Information, Communication & Society*, vol. 23, núm. 8, 2020, pp. 1139-1153.

[32] CASAROSA, «Cybersecurity of Internet of Things in the health sector: Understanding the applicable legal framework», *Computer Law & Security Review*, vol. 53, 2024, pp. 3-6.

[33] Reglamento (UE) 2025/327 del Parlamento Europeo y del Consejo, de 11 de febrero de 2025, relativo al Espacio Europeo de Datos de Salud y por el que se modifican la Directiva 2011/24/UE y el Reglamento (UE) 2024/2847, arts. 61, 68 y 73; vid. también considerandos 70 a 72.

persona, pero no elimina el carácter personal del dato cuando la reidentificación sigue siendo posible mediante información adicional o cruces con otros conjuntos. Por ello, la reutilización de datos de salud exige no solo técnicas de separación o codificación, sino también reglas de finalidad, seguridad, trazabilidad y control sobre ulteriores transferencias[34].

La infraestructura técnica sobre la que descansará el EEDS obliga también a mirar más allá del responsable formal. La contratación de servicios en la nube, la intervención de encargados y subencargados, la eventual transferencia internacional de información y el uso de arquitecturas distribuidas pueden diluir la identificación del sujeto que decide o ejecuta el tratamiento. Desde el Derecho civil, esta complejidad no puede operar en perjuicio del afectado. La trazabilidad debe alcanzar a toda la cadena técnica y contractual, y, cuando la reutilización se apoye en analítica de datos masivos, el sistema debe permitir reconstruir las operaciones relevantes y facilitar la prueba del origen del daño. Los comités de ética y las estructuras de revisión de proyectos de investigación no pueden limitarse a comprobar formularios de consentimiento: deben valorar anonimización, seudonimización, cruces de bases de datos, externalización tecnológica, finalidad científica real y riesgos de comercialización encubierta[35].

La literatura técnica ha demostrado que la anonimización no siempre cumple la promesa de irreversibilidad. OHM advirtió ya que la anonimización podía generar una falsa sensación de seguridad en contextos de cruce de bases de datos[36]. De igual manera, ROCHER, HENDRICKX Y DE MONTJOYE han mostrado que conjuntos incompletos pueden seguir siendo reidentificables mediante modelos generativos y datos auxiliares[37].

En el ámbito genómico, la advertencia es todavía más intensa. Gymrek et al. demostraron la posibilidad de inferir apellidos desde genomas personales mediante perfiles Y-STR y bases genealógicas recreativas[38]. Asimismo, SHRINGARPURE y BUSTAMANTE han analizado riesgos de privacidad en sistemas de compartición de datos genómicos capaces de revelar pertenencia a un conjunto y rasgos fenotípicos inferidos[39]. Por lo tanto, cuando el EEDS admite la reutilización de datos genéticos o de enfermedades raras, la tutela civil no puede descansar en la simple afirmación de que los datos han sido tratados técnicamente.

[34] PENASA *et al.*, «The EU General Data Protection Regulation: How will it impact the regulation of research biobanks? Setting the legal frame in the Mediterranean and Eastern European area», *Medical Law International*, vol. 18, núm. 4, 2018, pp. 241-255.

[35] NAVAS NAVARRO, «Computación en la nube: Big Data y protección de datos personales», *InDret*, núm. 4, 2015, pp. 1-48; MARTIN JIMÉNEZ, «Big Data: riesgos y soluciones desde el Derecho y desde los principios», *Revista de Derecho Politico*, núm. 119, 2024, pp. 215-249; SIMÓN MARCO, «Evolución del derecho a la protección de datos y disrupción tecnológica: ¿estamos vallando el campo?», *Revista CEFLegal*, núm. 233, 2020, pp. 89-120; DE LECUONA, «Evaluación de los aspectos metodológicos, éticos, legales y sociales de proyectos de investigación en salud con datos masivos (big data)», *Gaceta Sanitaria*, vol. 32, núm. 6, 2018, pp. 576-578.

[36] OHM, «Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization», *UCLA Law Review*, vol. 57, 2010, pp. 1704-1711.

[37] ROCHER/ HENDRICKX/DE MONTJOYE, «Estimating the Success of Re-identifications in Incomplete Datasets Using Generative Models», *Nature Communications*, vol. 10, 2019, art. 3069, pp. 1-9.

[38] GYMREK/MCGUIRE/GOLAN/HALPERIN/ERLICH, «Identifying Personal Genomes by Surname Inference», *Science*, vol. 339, núm. 6117, 2013, pp. 321-324.

[39] SHRINGARPURE/BUSTAMANTE, «Privacy Risks from Genomic Data-Sharing Beacons», *American Journal of Human Genetics*, vol. 97, núm. 5, 2015, pp. 631-646.

Desde la responsabilidad civil, hay que distinguir tres escenarios. El primero es la brecha de seguridad: acceso, exfiltración o difusión no autorizada de datos de salud. El segundo es la reidentificación: reasociación de un dato seudonimizado o aparentemente anonimizado con una persona concreta. El tercero es la inferencia algorítmica: obtención de información sanitaria sensible a partir de cruces de datos o modelos predictivos. Los tres pueden generar daño moral, pérdida de control y, en ocasiones, perjuicio patrimonial. El tercer escenario –la inferencia algorítmica– merece una atención específica porque representa el desafío civil más novedoso y menos explorado. A diferencia de la brecha de seguridad o de la reidentificación, la inferencia no presupone un acceso indebido ni la reasociación de un dato con su titular. Opera sobre datos en apariencia lícitamente tratados para deducir información que el sujeto nunca proporcionó expresamente. Un sistema de inteligencia artificial entrenado con historias clínicas puede inferir, a partir de patrones combinados, predisposiciones genéticas, trastornos mentales latentes, comportamientos adictivos o expectativas vitales, sin que ningún dato concreto sea, aisladamente, sensible. Como han puesto de relieve Wachter y Mittelstadt, la inferencia genera lo que denominan «datos derivados» (*inferred data*), que no son recogidos sino construidos por el sistema, y que pueden ser más reveladores e íntimos que los datos originales[40]. Esta construcción algorítmica de información sanitaria plantea un problema civil de primera magnitud: ¿quién es responsable cuando el dato inferido es erróneo y causa daño?, ¿quién responde cuando el dato inferido es correcto pero su obtención viola las expectativas razonables de privacidad del paciente? A nuestro juicio, ambas preguntas deben tener respuesta civil, no solo administrativa. El artículo 22 RGPD ofrece un punto de partida en materia de decisiones automatizadas individuales, pero no agota el problema: la inferencia masiva sin decisión individual identificable escapa de su ámbito de aplicación estricto. Por ello, BYGRAVE ha sostenido que el RGPD presenta una laguna estructural en materia de datos inferidos que los ordenamientos nacionales deben colmar[41]. La futura legislación española de salud digital debería afrontar expresamente esta laguna, estableciendo que la creación de perfiles de salud basados en inferencias algorítmicas genera, por sí misma, los mismos deberes de información, limitación de finalidad y responsabilidad por daños que el tratamiento de datos de salud expresamente declarados.

El daño moral sanitario presenta una intensidad propia. La exposición de datos financieros puede ser grave, la exposición de datos de salud puede afectar la identidad personal, la reputación, la vida familiar, la empleabilidad, la asegurabilidad y la confianza en el sistema sanitario. Además, el daño puede ser irreversible: una vez revelada una patología, una predisposición genética o un dato psiquiátrico, la reparación económica no recompone plenamente la esfera de privacidad perdida. Por ello, la tutela civil debe operar de forma preventiva y reparadora.

A nuestro juicio, la pérdida de control debe ser reconocida como una modalidad relevante de daño no patrimonial cuando afecte a datos de salud. No toda infracción formal debe generar automáticamente indemnización, pero tampoco puede exigirse al afectado que demuestre una consecuencia psicológica extrema. En materia sanitaria, la angustia razonable, la incertidumbre sobre el destino de datos íntimos y la exposición a usos discriminatorios constituyen efectos jurídicamente relevantes si se apoyan en hechos objetivos.

[40] WACHTER/MITTELSTADT, «A right to reasonable inferences: re-thinking data protection law in the age of big data and AI», *Columbia Business Law Review*, vol. 2019, núm. 2, 2019, pp. 494-620.

[41] BYGRAVE, *Data Privacy Law: An International Perspective*, Oxford University Press, Oxford, 2014, pp. 62-89.

La jurisprudencia del Tribunal de Justicia de la Unión Europea sobre el artículo 82 RGPD ofrece criterios particularmente útiles para delimitar el daño indemnizable. En el asunto *Österreichische Post*, el TJUE afirmó, por un lado, que la mera infracción del RGPD no basta por sí sola para generar un derecho a indemnización y, por otro, que el daño moral no puede quedar condicionado a la superación de un umbral mínimo de gravedad[42]. Asimismo, en el asunto VB c. *Natsionalna agentsia za prihodite*, admitió que el temor fundado a un posible uso indebido de los datos personales por terceros puede constituir un daño moral indemnizable[43].

La jurisprudencia civil española ha acogido en los últimos años estos criterios europeos sobre el daño indemnizable en el marco del RGPD. Así, la STS 398/2024, Civil, de 19 de marzo de 2024, ha precisado que no toda infracción de la normativa de protección de datos comporta necesariamente una vulneración del derecho a la intimidad y que, para que nazca el derecho a indemnización, es necesaria la existencia de un perjuicio real[44]. Esta doctrina, coherente con la sentada por el TJUE en *Österreichische Post*, plantea una dificultad específica cuando se proyecta sobre los datos de salud. La opacidad técnica de los sistemas interoperables, la pluralidad de sujetos que intervienen en el ecosistema del EEDS y la frecuente invisibilidad inicial del daño para el afectado pueden convertir la exigencia de prueba del perjuicio real en un obstáculo estructural para el ejercicio de la acción civil.

5. Responsabilidad civil por tratamiento ilícito, brecha de seguridad o reidentificación

Los tres escenarios generadores de daño identificados en el epígrafe anterior –brecha de seguridad, reidentificación e inferencia algorítmica– exigen ahora un análisis sistemático del régimen de responsabilidad civil aplicable, distinguiendo con nitidez la conducta que genera el daño, ya descrita, del daño indemnizable y del régimen de imputación, que se abordan a continuación. La responsabilidad civil en el EEDS debe cumplir una función doble. En primer lugar, una función reparadora: compensar a la persona afectada por daños materiales y morales. En segundo lugar, una función preventiva: incentivar diligencia reforzada en quienes tratan datos especialmente sensibles. En nuestra opinión, si el sistema permite una circulación ampliada de datos, debe asumir también una ampliación correlativa de los deberes de seguridad, transparencia y reparación.

5.1. El artículo 82 RGPD y el artículo 100 EEDS

La reparación de los daños derivados del tratamiento de datos de salud se sitúa en la confluencia del RGPD, el EEDS y el Derecho civil interno. El artículo 82 RGPD reconoce que toda persona que haya sufrido daños materiales o inmateriales como consecuencia de una infracción del Reglamento tendrá derecho a recibir del responsable o del encargado una indemnización por los

[42] STJUE de 4 de mayo de 2023, UI c. *Österreichische Post AG*, C-300/21, ECLI:EU:C:2023:370, UI c. *Österreichische Post AG*, apartados 32, 42 y 51.

[43] STJUE de 14 de diciembre de 2023, VB c. *Natsionalna agentsia za prihodite*, C-340/21, ECLI:EU:C:2023:986, 79 a 86.

[44] STS 398/2024, Civil, de 19 de marzo de 2024 (ECLI:ES:TS:2024:1495).

daños sufridos[45]. Este precepto ha sido esencial para europeizar la responsabilidad por daños de protección de datos. Por su parte, el artículo 100 del Reglamento relativo al EEDS dispone, de forma paralela, que toda persona física o jurídica que haya sufrido daños materiales o morales como consecuencia de una infracción del Reglamento tiene derecho a recibir indemnización conforme al Derecho de la Unión y nacional[46]. La existencia del precepto impide afirmar que el Reglamento ignore totalmente la reparación. Sin embargo, su formulación es demasiado escueta y, como señala RUBÍ PUIG, «los afectados no podrán fundar sus pretensiones indemnizatorias en este precepto, sino que deberán identificar otro fundamento en el derecho europeo o en el derecho nacional para sustentar una acción indemnizatoria»[47]. Esto es así porque no establece criterios propios de imputación, no define reglas probatorias específicas, no prevé un fondo de compensación, no configura presunciones de daño en supuestos graves y no desarrolla una vía procedimental especializada. Además, esta remisión podría ser insuficiente por tres razones: en primer lugar, el ciudadano normalmente desconoce qué entidad gestionó el dato, qué organismo autorizó el acceso, qué usuario lo trató y dónde se produjo la brecha. En segundo lugar, la prueba técnica del incumplimiento suele estar en manos de quienes integran el ecosistema de datos y, en tercer lugar, el daño moral sanitario puede no manifestarse de forma inmediata, aunque la pérdida de control sea ya objetivamente relevante.

En el Derecho español, las vías generales serían la responsabilidad contractual, cuando exista una relación asistencial o de prestación de servicios, y la responsabilidad extracontractual del artículo 1902 del Código civil cuando la lesión provenga de un tercero ajeno a la relación previa; e incluso la vía de la responsabilidad patrimonial de la Adminsitración, en aquellos casos en los que el daño se provoque como consecuencia de la actividad pública. También podrían operar acciones vinculadas a la protección civil del honor, intimidad y propia imagen, en función del tipo de intromisión[48]. No obstante, estos cauces generales no siempre se adaptan bien a daños digitales complejos, transfronterizos y técnicamente opacos.

Adicionalmente, el artículo 101 EEDS contempla mecanismos de representación de personas físicas cuando consideren infringidos sus derechos, lo que puede favorecer reclamaciones colectivas o por entidades habilitadas[49]. Sin embargo, tampoco esta previsión sustituye la

[45] RGPD, art. 82.1. Sobre su relación con el EEDS, vid. Reglamento (UE) 2025/327, art. 100 (derecho a recibir una indemnización cuando cualquier persona «física o jurídica» sufra «daños materiales o morales» como consecuencia de una infracción del Reglamento).

[46] *Vid.,* ampliamente, RUBÍ PUIG, «Espacio Europeo de Datos de Salud y responsabilidad civil. La norma indemnizatoria del artículo 100 del Reglamento (UE) 2025/327», en MORENO MARTÍNEZ (coord.), *Uso de Inteligencia Artificial en la Cirugía 4.0 y Salud Digital: Incidencias Jurídicas –Perspectivas Tecnológicas, Médicas y Legales–,* Dykinson, Madrid, 2026, pp. 877-928. El autor explica que el artículo 100 REEDS consagra una norma de garantía indemnizatoria imperfecta, que no crea una acción autónoma, sino que remite a otros fundamentos del Derecho de la UE o nacional (especialmente el art. 82 RGPD) para reclamar la reparación de daños materiales o morales derivados de infracciones del Reglamento. La legitimación activa corresponde a personas físicas y jurídicas, la pasiva, a autoridades de salud digital, organismos de acceso, tenedores y usuarios de datos. La eficacia práctica del precepto –que se complementa con el considerando 101, sobre la reparación integral y la interpretación amplia del daño, y con las normas sectoriales sobre uso primario, secundario y seguridad de sistemas de HCE– dependerá de la articulación con los regímenes internos de responsabilidad, sin perjuicio del control del TJUE sobre su interpretación uniforme.

[47] *Ibid*., pág. 924.

[48] Código civil, art. 1902. *Vid*. también Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, arts. 1, 2, 7 y 9.

[49] Por el que se abre la puerta a las acciones de representación cuando el perjudicado considere que se le han vulnerado los derechos que le reconoce el Reglamento relativo al EEDS.

necesidad de un régimen civil materialmente eficaz. La representación facilita el ejercicio de la acción, pero no resuelve por sí sola los problemas de prueba, cuantificación, identificación del responsable y ejecución transfronteriza.

5.2. Sujetos responsables y deberes reforzados de diligencia

El ecosistema del EEDS multiplica los sujetos relevantes. Intervienen prestadores sanitarios, tenedores de datos, organismos de acceso a datos de salud, usuarios de datos, encargados del tratamiento, proveedores tecnológicos, operadores de entornos seguros y autoridades supervisoras. Esta pluralidad puede mejorar la gobernanza, pero también puede diluir la responsabilidad. Desde el Derecho civil, la complejidad organizativa no debe convertirse en una excusa para la irresponsabilidad.

Conviene precisar, además, qué sujetos del ecosistema del EEDS pueden quedar sometidos al artículo 82 RGPD. Dicho precepto se aplica a quienes ostentan la condición de responsable o encargado del tratamiento en el sentido del RGPD: típicamente, el prestador sanitario, el organismo de acceso a datos de salud y, en su caso, el usuario de datos cuando trata datos personales para fines de investigación u otros usos secundarios. La cuestión es más dudosa respecto de los operadores de entornos seguros de tratamiento y de los proveedores tecnológicos que actúan como meros encargados sin margen de decisión sobre los fines y medios del tratamiento: estos últimos podrán no responder directamente frente al paciente al amparo del artículo 82 RGPD, sin perjuicio de su responsabilidad interna frente al responsable. El artículo 100 EEDS, por su parte, reconoce el derecho a indemnización mediante una remisión al Derecho de la Unión y al Derecho nacional, sin sustituir el régimen del artículo 82 RGPD ni resolver expresamente qué ocurre con aquellos sujetos del EEDS que, no siendo responsables ni encargados en sentido RGPD, intervienen materialmente en el ecosistema –así, determinados organismos de gobernanza o infraestructuras técnicas compartidas– y, como afirma RUBÍ PUIG, «el artículo 82 RGPD, tal como viene siendo interpretado por el TJUE, constituiría probablemente el marco principal para dilucidar la reparación de los daños y perjuicios en el ámbito del EEDS»[50].

De lege ferenda, sería deseable que la futura Ley española de Salud Digital precisara el régimen de responsabilidad aplicable a estos últimos sujetos, bien mediante su equiparación funcional a los encargados del tratamiento, bien mediante un régimen específico de responsabilidad objetiva o cuasi objetiva por el riesgo creado[51]. La regla debe ser la diligencia reforzada. Quien trata datos

[50] RUBÍ PUIG, «Espacio Europeo de Datos de Salud y responsabilidad civil. La norma indemnizatoria del artículo 100 del Reglamento (UE) 2025/327», en MORENO MARTÍNEZ (coord.), *Uso de Inteligencia Artificial en la Cirugía 4.0 y Salud Digital: Incidencias Jurídicas –Perspectivas Tecnológicas, Médicas y Legales–*, Dykinson, Madrid, 2026, p. 924.

[51] *N. B.* El régimen del artículo 82 RGPD ofrece, además, herramientas específicas para la pluralidad de sujetos característica del EEDS. En primer lugar, su apartado 3 exonera de responsabilidad al responsable o encargado que demuestre no ser en modo alguno responsable del hecho que originó el daño -exoneración que, en el EEDS, exigirá acreditar el cumplimiento estricto de los protocolos de acceso, trazabilidad y seguridad propios de cada rol-. En segundo lugar, su apartado 4 establece que, cuando varios responsables o encargados –o un responsable y un encargado– hayan participado en el mismo tratamiento y sean responsables de un daño, cada uno de ellos responderá de la totalidad del daño, precisamente para garantizar una indemnización efectiva del interesado. Esta regla resulta especialmente valiosa en el EEDS, donde la intervención simultánea de tenedores de datos, organismos de acceso y usuarios de datos dificulta aislar la contribución causal de cada uno. Y, finalmente, su apartado 5 reconoce el correlativo derecho de regreso: quien haya satisfecho la totalidad de la indemnización podrá reclamar de los demás responsables o encargados implicados la parte que corresponda a su respectiva responsabilidad en el daño causado. Sin embargo, la articulación de este régimen con el artículo 100 EEDS no es

de salud no cumple con una diligencia ordinaria, sino con una diligencia cualificada por la sensibilidad del dato, la previsibilidad del daño y la intensidad de los riesgos. BLÁZQUEZ RUIZ ha advertido que las garantías constitucionales de privacidad requieren mecanismos robustos de rendición de cuentas frente a quienes abusan o se lucran con datos personales obtenidos ilícitamente[52]. De igual modo, la responsabilidad civil debe traducir esa rendición de cuentas en deberes concretos de identificación, seguridad, trazabilidad y reparación.

La diligencia reforzada exige, al menos, una evaluación previa del riesgo antes de poner los datos a disposición para usos secundarios, la estricta minimización de los datos que circulan, la adopción de medidas de seguridad técnica actualizadas –incluidos cifrado, control de accesos, registro de operaciones y auditorías periódicas–, la trazabilidad completa de cada acceso, con identificación del sujeto que accede, del momento, de la finalidad y del permiso habilitante, y, finalmente, una respuesta rápida ante incidentes, acompañada de información efectiva al afectado y de mecanismos de reclamación accesibles.

La responsabilidad civil debe adaptarse a esta estructura: si un organismo autoriza indebidamente un acceso, si un tenedor entrega datos más amplios de los necesarios, si un usuario excede la finalidad autorizada o si un proveedor tecnológico incumple medidas de seguridad, cada sujeto debe responder en función de su intervención causal y de su esfera de control. Debe advertirse, no obstante, que este régimen de responsabilidad extracontractual del artículo 1902 CC solo opera cuando el prestador sanitario es una entidad privada. Cuando el prestador es un servicio público de salud, el paciente no dispone de la acción del artículo 1902 CC, sino de la acción de responsabilidad patrimonial de la Administración, con sus propios presupuestos, plazo de prescripción y vía de reclamación previa, lo que introduce una dualidad de regímenes de responsabilidad –contractual o extracontractual, de un lado, y patrimonial-administrativa, de otro– que la futura Ley española de Salud Digital debería coordinar expresamente para evitar desigualdades de tutela entre pacientes de la sanidad pública y de la privada. Asimismo, cuando la opacidad del sistema impida al afectado identificar el origen exacto del daño, de lege ferenda debería reconocerse la operatividad de reglas de solidaridad o de distribución interna de responsabilidad entre los intervinientes, pues el Derecho vigente no articula todavía un mecanismo específico para esta hipótesis.

De ahí que resulte razonable defender una carga dinámica de la prueba. Por ello, propugnamos de lege ferenda la corrección de la asimetría probatoria mediante una carga dinámica de la prueba –que debería desplazar al responsable la acreditación de la diligencia desplegada y de la ausencia de daño indemnizable en supuestos de brecha grave, reidentificación o incumplimiento de trazabilidad– ofrece una respuesta concreta al problema identificado tanto por la jurisprudencia nacional como por el propio TJUE. Estas ideas deben proyectarse, con mayor razón, sobre los datos relativos a la salud de los ciudadanos. Corresponde al afectado acreditar un daño o, al menos, una lesión objetivable de su esfera de control. Pero corresponde a quienes gestionan el sistema probar que actuaron con la diligencia debida, que el acceso estaba autorizado, que el

automática: este último remite al «Derecho de la Unión» y al Derecho «nacional» sin aclarar si la responsabilidad solidaria del artículo 82.4 RGPD se extiende a los sujetos del EEDS (que no ostentan la condición de «responsable» o «encargado» en sentido del RGPD). Resulta necesario que esta cuestión sea abordada pertinentemente por la futura Ley española de Salud Digital, que debería resolverla expresamente.

[52] BLÁZQUEZ RUIZ, «Aplicaciones de la inteligencia artificial al ámbito biosanitario: protección de datos y privacidad. Implicaciones éticas y legales», *Anales de la Cátedra Francisco Suárez*, núm. 56, 2022, p. 264.

tratamiento fue proporcional y que las medidas de seguridad eran adecuadas al riesgo. Por consiguiente, la asimetría informativa debe corregirse en el plano probatorio.

La trazabilidad debería erigirse, de lege ferenda, en una garantía civil autónoma –hoy no reconocida expresamente como tal en nuestro ordenamiento–. No serviría solo para auditorías administrativas, serviría para identificar responsables, reconstruir causalidad y cuantificar daños. Sin registros fiables de acceso y tratamiento, la acción civil se vuelve prácticamente ilusoria. Por ello, a nuestro juicio, la futura Ley española de Salud Digital debería concebir la trazabilidad no solo como requisito técnico, sino como presupuesto de tutela judicial efectiva en materia de daños sanitarios digitales.

La diligencia reforzada no se agota, por tanto, en impedir accesos no autorizados. Comprende también deberes de calidad, coherencia semántica, actualización y validación de los datos puestos a disposición para usos secundarios. Un dato clínico técnicamente accesible, pero incompleto, mal codificado o descontextualizado, puede generar riesgos propios: inferencias erróneas, resultados algorítmicos sesgados, conclusiones científicas defectuosas o decisiones sanitarias indirectamente lesivas. Cuanto mayor sea la escala de reutilización y más intensa la automatización del análisis, más exigible será que quienes custodian, describen o autorizan el uso de los datos puedan acreditar la idoneidad del conjunto utilizado para la finalidad declarada[53].

Esta exigencia se intensifica cuando los datos de salud sirven para entrenar, validar o alimentar sistemas de inteligencia artificial con impacto clínico. En tales casos, el riesgo no se limita a la privacidad, sino que puede proyectarse sobre la propia asistencia sanitaria. La diligencia exigible debe comprender la validación del sistema en un entorno comparable al de uso, la integración segura con la historia clínica, la supervisión humana efectiva, la documentación de la intervención algorítmica y la posibilidad real de corregir o rechazar la recomendación automatizada. Si la herramienta influye de forma relevante en el diagnóstico, la priorización o el tratamiento, el paciente debe conservar también un derecho material a comprender que ha existido esa intervención y a exigir una explicación suficiente[54].

5.3. Daño moral, prueba y causalidad

La cuestión más delicada es la prueba del daño moral. En materia de datos de salud, no debería exigirse al afectado una prueba psicológica excesiva cuando la lesión objetiva sea grave. La exposición no autorizada de una enfermedad, de un diagnóstico psiquiátrico, de un dato genético o de información reproductiva puede lesionar la intimidad por sí misma. También puede generar

[53] LAZCOZ MORATINOS/DE MIGUEL BERIAIN, «Is more data always better? On alternative policies to mitigate bias in Artificial Intelligence health systems», *Bioethics,* vol. 39, núm. 5, 2025, pp. 414-424; DE MIGUEL BERIAIN, «Medicina personalizada, algoritmos predictivos y utilización de sistemas de decisión automatizados en asistencia sanitaria. Problemas éticos», *Dilemata. Revista Internacional de Éticas Aplicadas*, núm. 30, 2019, pp. 93-109.

[54] DE MIGUEL BERIAIN, «La aplicabilidad del Reglamento de inteligencia artificial al ámbito salud y especialidades respecto de su cumplimiento», en COTINO HUESO/SIMÓN CASTELLANO (dirs.), *Tratado sobre el Reglamento de Inteligencia Artificial de la Unión Europea*, 2024, pp. 337-348. *Cfr.* LAZCOZ MORATINOS, «La vigilancia o supervisión humana en el artículo 14 del Reglamento de inteligencia artificial: ¿un mero requisito obligatorio para los sistemas de alto riesgo?», en COTINO HUESO/SIMÓN CASTELLANO (dirs.), *Tratado sobre el Reglamento de Inteligencia Artificial de la Unión Europea,* 2024, pp. 681-699.

miedo, vergüenza, estigmatización, pérdida de confianza y alteración de la vida personal o familiar.

El Tribunal de Justicia ha rechazado la existencia de un umbral mínimo de gravedad para el daño moral indemnizable del RGPD, aunque exige que el daño sea real y probado[55], doctrina reafirmada en 2025 al calificar la pérdida de control sobre los propios datos como un perjuicio inmaterial autónomo, reparable con independencia de cualquier umbral de gravedad[56]. En nuestra opinión, esta doctrina permite construir una regla equilibrada para datos de salud: no toda irregularidad formal genera indemnización automática, pero, de lege ferenda, proponemos que ciertas lesiones graves de control, confidencialidad o seguridad justifiquen una presunción razonable de daño moral, salvo prueba en contrario, sin que ello implique afirmar que tal presunción esté ya reconocida en el Derecho vigente.

Esta presunción sería especialmente justificada en tres supuestos: brecha grave de seguridad con acceso no autorizado a datos clínicos identificables, reidentificación de datos seudonimizados o aparentemente anonimizados, y uso de datos de salud para finalidades prohibidas o discriminatorias. También debería operar cuando el afectado no pueda conocer el alcance exacto de la difusión porque el responsable no conserva registros suficientes. No puede premiarse probatoriamente a quien incumple deberes de trazabilidad.

La causalidad presenta dificultades particulares. En un ecosistema interoperable, el daño puede resultar de una cadena de decisiones: recogida del dato, conservación, seudonimización defectuosa, autorización insuficiente, acceso excesivo, ausencia de controles y uso posterior. Por ello, el análisis causal debe atender a la posición de garante de cada interviniente. Quien crea o administra un riesgo digital significativo debe responder por las consecuencias previsibles de su materialización si no acredita haber adoptado medidas razonables.

La cuantificación debe atender a criterios como la naturaleza del dato, número de accesos, duración de la exposición, grado de identificabilidad, finalidad del tratamiento, vulnerabilidad del afectado, reiteración del incumplimiento, conducta posterior del responsable y medidas de mitigación. Asimismo, debe valorarse si el dato afectaba a enfermedad estigmatizante, salud mental, genética, salud sexual o información relativa a menores. Del mismo modo, la indemnización debe cumplir una función suficientemente disuasoria para que la tutela civil no sea absorbida por el coste ordinario de la actividad.

La coordinación con las sanciones administrativas es imprescindible. Una multa puede castigar el incumplimiento, pero no repara a la persona. Además, la existencia de sanción no debe impedir la reclamación civil, más bien puede servir como elemento probatorio del incumplimiento. A nuestro juicio, la resolución administrativa firme debería tener una eficacia relevante en el proceso civil, al menos respecto de los hechos constatados y la infracción declarada, sin perjuicio de la prueba del daño y de la causalidad.

[55] STJUE 4 mayo 2023, asunto C-300/21, UI c. *Österreichische Post* AG, apartados 50 y 51. En sentido complementario, STJUE de 25 de enero de 2024, BL c. *MediaMarktSaturn Hagen-Iserlohn GmbH*, C-687/21, ECLI:EU:C:2024:72, apartados 60 a 67.

[56] STJUE de 4 de septiembre de 2025, *Quirin Privatbank*, C-655/23, ECLI:EU:C:2025:655, apartados 55 y 56.

Cabe plantearse, finalmente, si la indemnización civil en materia de datos de salud debe cumplir únicamente una función compensatoria o si puede incorporar, en determinados supuestos, una dimensión punitiva o desincentivadora suficientemente intensa. La cuestión es polémica en el Derecho continental, donde los daños punitivos carecen de reconocimiento expreso en el ordenamiento español. Sin embargo, la doctrina más atenta a los daños digitales ha señalado que la cuantificación meramente reparadora puede resultar insuficiente cuando el responsable haya obtenido beneficios derivados del tratamiento ilícito superiores a la indemnización pagada, o cuando la probabilidad de ser identificado y demandado sea estadísticamente baja, lo que convierte la responsabilidad en un coste tolerable de la actividad. Koziol ha argumentado que las funciones preventiva y sancionadora de la responsabilidad civil, aunque secundarias en la tradición continental, adquieren mayor relieve cuando el daño afecta a bienes de la personalidad y cuando la asimetría entre dañante y dañado hace inviable la tutela puramente compensatoria[57]. En este marco, aunque no corresponda hablar de daños punitivos en sentido estricto, la jurisprudencia española podría desarrollar un criterio de cuantificación del daño moral que tome en consideración el beneficio obtenido por el infractor, la reiteración de la conducta, la posición de poder del responsable y la particular vulnerabilidad de los datos afectados. Esta orientación encuentra apoyo en la Directiva (UE) 2020/1828 sobre acciones de representación, que promueve que la reparación colectiva sea efectiva y disuasoria[58], y podría proyectarse sobre acciones colectivas en materia de brechas masivas de datos sanitarios, en las que la lesión individual es difusa pero el daño social es considerable.

6. La futura Ley española de Salud Digital

El proceso español de elaboración de la futura Ley de Salud Digital ofrece una ocasión especialmente relevante para integrar la dimensión iusprivatista del EEDS. La norma no debería limitarse a organizar la interoperabilidad, crear autoridades o reproducir categorías europeas. Debe preguntarse también qué remedios tendrá el ciudadano si el sistema falla. En nuestra opinión, esta es la verdadera prueba de madurez de la digitalización sanitaria: no solo funcionar, sino responder.

La descentralización sanitaria española añade complejidad. Las comunidades autónomas gestionan servicios sanitarios y sistemas de información con distintos grados de madurez. La futura historia clínica digital interoperable debe operar en todo el territorio y, además, integrar a prestadores privados. PERNA, CRUZ-MARTÍNEZ y MORENO FUENTES han analizado cómo la movilidad de pacientes y la descentralización sanitaria plantean retos específicos para el Sistema Nacional de Salud[59]. Igualmente, la gobernanza de datos exigirá coordinación técnica y jurídica para que la protección civil no varíe según territorio.

La estructura federada del futuro espacio nacional refuerza esta exigencia. Si los datos no se integran en un repositorio único, sino que permanecen en distintos sistemas conectados

[57] KOZIOL, «Punitive Damages: Admission into the Club*?», Journal of European Tort Law*, vol. 1, núm. 1, 2010, pp. 9-37. DOI: https://doi.org/10.1515/JETL.2010.9.

[58] Directiva (UE) 2020/1828 del Parlamento Europeo y del Consejo, de 25 de noviembre de 2020, relativa a las acciones de representación para la protección de los intereses colectivos de los consumidores. DOUE L 409, de 4 de diciembre de 2020.

[59] PERNA/CRUZ-MARTÍNEZ/MORENO FUENTES, «Movilidad de pacientes y descentralización sanitaria: respuestas y retos en el Sistema Nacional de Salud español», *Gestión y Análisis de Políticas Públicas*, núm. 30, 2022, pp. 27-44, especialmente pp. 31-37.

mediante protocolos comunes, la garantía civil no puede depender del nodo desde el que se produzca el acceso, de la comunidad autónoma que custodie la información o del grado de madurez tecnológica de cada plataforma. La futura Ley debería establecer un suelo común de protección aplicable a todos los participantes: registro completo de accesos, trazabilidad interoperable, criterios homogéneos de notificación de incidencias, ejercicio portable del derecho de autoexclusión y un canal claro para que el ciudadano pueda identificar frente a quién debe reclamar[60].

La perspectiva civil aconseja introducir, al menos, ocho previsiones. La primera es un mecanismo nacional de opt-out único, accesible, comprensible, reversible y operativo frente a prestadores públicos y privados. La segunda es un deber reforzado de información al ciudadano, con lenguaje claro y explicación de las finalidades de uso secundario. La tercera es una obligación de trazabilidad individualizada que permita conocer accesos, permisos, usuarios y finalidades. La cuarta previsión debería ser una regla probatoria específica. En caso de brecha grave, reidentificación o incumplimiento de trazabilidad, correspondería al responsable acreditar la diligencia desplegada y la ausencia de daño indemnizable. La quinta previsión sería una vía de reclamación civil ágil, especializada y coordinada con la Agencia Española de Protección de Datos y con los órganos de acceso a datos de salud. La sexta consistiría en reconocer expresamente la posibilidad de daño moral por pérdida objetiva de control sobre datos sanitarios especialmente sensibles. La séptima previsión debería consistir en una regla específica de gobernanza multinivel. La futura ley debe prever cómo se articulan los organismos de acceso a datos de salud, los servicios autonómicos, los prestadores privados, los comités éticos y las autoridades de protección de datos. La experiencia del Mercado Único Digital demuestra que la armonización normativa pierde eficacia si no se acompaña de una participación real de los niveles subestatales y de mecanismos de coordinación que eviten asimetrías territoriales en la disponibilidad y calidad de los datos[61]. La octava previsión debería conectar expresamente el modelo español con la gobernanza europea del EEDS. El Consejo del EEDS ha sido configurado como foro de cooperación entre Estados miembros y Comisión, con capacidad para emitir contribuciones escritas, guías de ejecución, directrices no vinculantes, hojas de ruta, estrategias de comunicación e intercambios de buenas prácticas, además, su funcionamiento se somete a reglas de secreto profesional, acceso documental y transparencia. La futura ley española debería prever un mecanismo interno para incorporar esas orientaciones al sistema nacional, publicarlas de modo comprensible, explicar su impacto sobre los derechos de los ciudadanos y evitar que la gobernanza técnica se desplace a espacios opacos sin rendición de cuentas[62]. Adicionalmente, la futura ley debería precisar la relación entre los organismos nacionales y regionales de acceso a datos de salud. Si la autorización se decide a nivel nacional, puede faltar conocimiento contextual sobre la procedencia y calidad del dato. Si se decide a nivel regional, puede surgir

[60] DE MIGUEL BERIAIN/LÓPEZ DE LA PEÑA DE PABLO/LOYO-MENOYO, «El nuevo reglamento europeo relativo al espacio europeo de datos de salud: su impacto en la gobernanza del dato y su uso ético y seguro», cit.; DE MIGUEL BERIAIN/ATIENZA-MACÍAS/ARMAZA ARMAZA, «The European Union Integrated Political Crisis Response Arrangements: Improving the European Union's Major Crisis Response Coordination Capacities», *Disaster Medicine and Public Health Preparedness,* vol. 9, núm. 2, 2015, pp. 234-238.

[61] RECUERO, «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», cit.; PÉREZ DE LAS HERAS, «Hacia el Mercado Único Digital en la Unión Europea: retos y potencialidades para los entes subestatales», *Ekonomiaz,* núm. 98, 2020, pp. 150-171.

[62] Reglamento de Ejecución (UE) 2026/771 de la Comisión, de 7 de abril de 2026, por el que se establecen las medidas necesarias para el establecimiento y el funcionamiento del Consejo del Espacio Europeo de Datos de Salud, considerandos 1 a 5 y arts. 2, 8, 9 y 10.

fragmentación y desigualdad. Por ello, parece preferible un modelo coordinado: decisión homogénea, intervención técnica regional cuando sea necesaria y registro nacional de permisos, accesos e incidencias.

También debe atenderse a la incorporación de tecnologías emergentes. La consulta pública ministerial menciona inteligencia artificial, biometría y neurotecnologías. Estas herramientas pueden mejorar diagnóstico y seguimiento, pero también intensificar la inferencia de información íntima. PÉREZ-UGENA ha advertido que la inteligencia artificial presenta riesgos significativos para los derechos fundamentales cuando opera mediante decisiones opacas o tratamientos masivos de datos[63]. Por consiguiente, la ley española debería prever garantías civiles frente a decisiones automatizadas o inferencias sanitarias perjudiciales. Entre esas tecnologías, los neurodatos merecen una mención específica. Su eventual integración en el EEDS no puede resolverse mediante una simple equiparación con otros datos sanitarios. Por su capacidad para revelar estados cognitivos, emocionales o conductuales, y por su posible utilización en el entrenamiento de sistemas de inteligencia artificial, deberían recibir una protección reforzada: exclusión de bases legitimadoras débiles cuando el acceso sea pretendido por usuarios privados, exigencia de motivación cualificada en el permiso de datos, posibilidad de consentimiento explícito para determinados usos secundarios y reconocimiento de un derecho de autoexclusión especialmente visible y granular[64].

No se trata, por lo tanto, de frenar la innovación. Se trata de disciplinarla jurídicamente. La investigación biomédica necesita datos, la medicina personalizada necesita interoperabilidad, la salud pública necesita información de calidad. Pero la persona necesita saber que no queda indefensa ante un ecosistema que no comprende. De la misma manera, el interés público no puede convertirse en una cláusula general de disponibilidad de la intimidad.

En este punto, la legislación civil y sanitaria debería asumir una idea de proporcionalidad material. Cuanto más sensible sea el dato, mayor debe ser la garantía. Cuanto más amplio sea el acceso, mayor debe ser la trazabilidad. Cuanto más opaco sea el sistema técnico, mayor debe ser la carga explicativa. Y cuanto más difícil sea para el afectado probar la lesión, más necesario será corregir la asimetría probatoria. Así entendido, el Derecho civil no obstaculiza el EEDS, lo legitima.

7. Conclusiones y propuestas de lege ferenda

Primera. El EEDS representa una oportunidad relevante para mejorar la asistencia sanitaria, la investigación biomédica y la formulación de políticas públicas. Su finalidad es legítima y responde a una necesidad real de interoperabilidad europea. Sin embargo, esa oportunidad no elimina la naturaleza civilmente sensible del dato de salud.

Segunda. La información sanitaria se integra en la esfera de los derechos de la personalidad. No es un dato neutro ni puramente administrativo. Puede afectar a la identidad, la reputación, la

[63] PÉREZ-UGENA, «La inteligencia artificial: definición, regulación y riesgos para los derechos fundamentales», *Estudios de Deusto. Revista de Derecho Público*, vol. 72, núm. 1, 2024, pp. 321-330.

[64] NAVAS NAVARRO, «Neurodatos y Espacio Europeo de Datos de Salud. Los "intereses legítimos" del usuario de datos», *Cuadernos de Derecho Privado*, núm. 14, 2026, pp. 139-173.

vida familiar, la empleabilidad, la asegurabilidad y la confianza en el sistema sanitario. Su reutilización exige garantías materiales, no solo gobernanza formal.

Tercera. El tránsito del consentimiento individual al modelo de autorización institucional con *opt-out* altera la posición jurídica del ciudadano. El derecho de autoexclusión puede ser una garantía útil, pero solo si es accesible, comprensible, reversible, granular y homogéneo. Un *opt-out* formalmente reconocido pero difícil de ejercer no satisface la exigencia civil de autonomía.

Cuarta. La ciberseguridad sanitaria debe formar parte del contenido de la diligencia civil exigible. En salud, una brecha de seguridad, una reidentificación o una inferencia algorítmica pueden producir daño moral, pérdida de control y perjuicios patrimoniales. La protección no puede descansar en la presunción de que la anonimización elimina todo riesgo.

Quinta. El artículo 100 EEDS reconoce el derecho a indemnización por daños materiales y morales, pero no establece un régimen civil reforzado. La futura legislación española debería concretar reglas de legitimación, prueba, trazabilidad, presunción de daño moral en supuestos graves y coordinación entre sanción administrativa e indemnización privada.

Sexta. A nuestro juicio, la tutela civil del EEDS debe construirse sobre una idea sencilla: la confianza ciudadana no nace de la mera interoperabilidad, sino de la posibilidad real de controlar, conocer y reparar. La innovación regulatoria solo será legítima si preserva la dignidad, la autonomía y la intimidad del paciente. En materia de datos de salud, la reparación efectiva no es un complemento del sistema, es una condición de su legitimidad.

Séptima. El éxito jurídico del EEDS no podrá medirse solo por la existencia de normas, autoridades y procedimientos de acceso. Desde el Derecho civil, la cuestión decisiva será si el sistema permite generar una confianza verificable: que el ciudadano pueda comprender el destino de sus datos, que los operadores puedan demostrar la licitud y diligencia de cada uso, que las incidencias sean trazables y que los daños encuentren una vía real de reparación. Sin esa dimensión probatoria y remedial, la interoperabilidad corre el riesgo de convertirse en una infraestructura eficiente para los usuarios de datos, pero insuficientemente protectora para quienes los originan.

Octava. Asimismo, el caso español puede aportar una respuesta relevante para otros Estados miembros. La descentralización del Sistema Nacional de Salud obliga a diseñar mecanismos de coordinación que permitan compatibilizar pluralidad institucional e igualdad de protección. Si España consigue articular un modelo de historia clínica interoperable, opt-out efectivo, trazabilidad y reparación civil reforzada, podrá ofrecer una pauta útil para la implementación nacional del EEDS en la Unión Europea.

Novena. De lege ferenda, la futura Ley española de Salud Digital debería convertir la trazabilidad en un derecho subjetivo operativo. No bastaría con registrar accesos para fines internos de auditoría: el ciudadano debe poder conocer, de forma comprensible, qué entidades han accedido a sus datos, con qué permiso, para qué finalidad y durante qué periodo, salvo límites estrictos, motivados y revisables. Esta información debería integrarse en una interfaz única para todo el Sistema Nacional de Salud y para los prestadores privados incorporados al ecosistema.

Décima. La ley debería establecer un estatuto civil del uso secundario de datos de salud. Ese estatuto tendría que incluir: opt-out nacional, multicanal y reversible, información reforzada sobre finalidades, categorías de datos y usuarios, reglas de granularidad para datos genéticos, biométricos, neurodatos, salud mental, enfermedades raras y menores, prohibición de invocar intereses puramente comerciales como justificación suficiente para acceder a datos especialmente sensibles, y obligación de motivar de forma reforzada todo permiso concedido a usuarios privados para entrenamiento o validación de sistemas de inteligencia artificial.

Undécima. La ley debería prever una regla específica de responsabilidad y prueba. En caso de brecha grave, reidentificación, incumplimiento del registro de accesos, uso fuera de finalidad o imposibilidad de reconstruir la cadena de tratamiento, debería presumirse la falta de diligencia del operador correspondiente, sin perjuicio de que este pueda acreditar que adoptó todas las medidas técnicas, organizativas y contractuales exigibles. Esta regla no eliminaría la necesidad de daño real, pero corregiría la asimetría probatoria que padece el paciente frente a infraestructuras de datos complejas.

Duodécima. Finalmente, la ley debería crear una vía de tutela civil especializada, sencilla y rápida, coordinada con la Agencia Española de Protección de Datos, los organismos de acceso a datos de salud y las autoridades sanitarias autonómicas. La digitalización sanitaria solo será legítima si el ciudadano puede reclamar sin tener que reconstruir por sí solo una cadena técnica que no controla. En ese punto se juega, en última instancia, la confianza civil del EEDS: que la interoperabilidad no deje al paciente más expuesto, sino mejor protegido.

8. Bibliografía

ÁLVAREZ OLALLA, María del Pilar, «El espacio europeo de datos de salud. Daños indemnizables», en HERRADOR GUARDIA, Mariano José (dir.), *Fundamentos, prueba y justicia del daño*, Aranzadi, Cizur Menor, 2026, pp. 561-594.

BLÁZQUEZ RUIZ, Francisco Javier, «Aplicaciones de la inteligencia artificial al ámbito biosanitario: protección de datos y privacidad. Implicaciones éticas y legales», *Anales de la Cátedra Francisco Suárez,* núm. 56, 2022, pp. 245-268.

BELTRÁN AGUIRRE, Juan Luis, «Tratamiento de datos de salud en la prestación de servicios sociales», *Derecho y Salud*, vol. 18, núm. 1, 2009, pp. 1-19.

BYGRAVE, Lee Andrew, *Data Privacy Law: An International Perspective*, Oxford University Press, Oxford, 2014.

CABALLERO TRENADO, Laura, «Cartografía legal de la autodeterminación informativa digital. Un derecho de construcción jurisprudencial», *Universitas*, núm. 35, 2021, pp. 2-27. DOI: https://doi.org/10.20318/universitas.2021.6189.

CADENAS OSUNA, Davinia, «El estándar de información sanitaria sobre riesgos de los tratamientos e intervenciones médicas en España y el common law: una visión panorámica», *InDret*, núm. 4, 2016, pp. 1-42.

CASANOVA ASENCIO, Andrea Salud, «Protección de datos en el ámbito de la historia clínica: el acceso indebido por el personal sanitario y sus consecuencias», *InDret,* núm. 2, 2019, pp. 1-31. https://indret.com/proteccion-de-datos-en-el-ambito-de-la-historia-clinica/.

CASAROSA, Federica, «Cybersecurity of Internet of Things in the health sector: Understanding the applicable legal framework», *Computer Law & Security Review*, vol. 53, 2024, pp. 1-12. https://doi.org/10.1016/j.clsr.2024.105982.

DE MIGUEL BERIAIN, Íñigo y LAZCOZ MORATINOS, Guillermo, «El Convenio de Oviedo, veinte años después de su firma. ALGUNAS sugerencias de enmienda», *Quaestio Iuris*, vol. 11, núm. 1, 2018, pp. 445-460. https://doi.org/10.12957/rqi.2018.31729.

DE MIGUEL BERIAIN, Íñigo/ATIENZA-MACÍAS, Elena/ARMAZA ARMAZA, Emilio, «The European Union Integrated Political Crisis Response Arrangements: Improving the European Union's Major Crisis Response Coordination Capacities», *Disaster Medicine and Public Health Preparedness*, vol. 9, núm. 2, 2015, pp. 234-238. DOI: https://doi.org/10.1017/dmp.2015.10.

DE MIGUEL BERIAIN, Íñigo, «MEDICINA PERSONALIZADA, ALGORITMOS PREDICTIVOS Y UTILIZACIÓN DE SISTEMAS DE DECISIÓN AUTOMATIZADOS EN ASISTENCIA SANITARIA. PROBLEMAS ÉTICOS», *Dilemata. Revista Internacional de Éticas Aplicadas*, núm. 30, 2019, pp. 93-109.

DE MIGUEL BERIAIN, Íñigo, «SHOULD WE HAVE A RIGHT TO REFUSE DIAGNOSTICS AND TREATMENT PLANNING BY ARTIFICIAL INTELLIGENCE?», *Medicine, Health Care and Philosophy*, vol. 23, 2020, pp. 247-252. DOI: https://doi.org/10.1007/s11019-020-09939-2.

DE MIGUEL BERIAIN, Íñigo /SANZ, Begoña/LAZCOZ MORATINOS, Guillermo, «MACHINE LEARNING IN THE EU HEALTH CARE CONTEXT: EXPLORING THE ETHICAL, LEGAL AND SOCIAL ISSUES», *Information, Communication & Society*, vol. 23, núm. 8, 2020, pp. 1139-1153. DOI: https://doi.org/10.1080/1369118X.2020.1719185.

DE MIGUEL BERIAIN, Íñigo, «LA APLICABILIDAD DEL REGLAMENTO DE INTELIGENCIA ARTIFICIAL AL ÁMBITO SALUD Y ESPECIALIDADES RESPECTO DE SU CUMPLIMIENTO», EN COTINO HUESO, LORENZO/SIMÓN CASTELLANO, PERE (DIRS.), *Tratado sobre el Reglamento de Inteligencia Artificial de la Unión Europea*, Aranzadi, Las Rozas, 2024, pp. 337-348.

DE MIGUEL BERIAIN, Íñigo, «Los derechos relativos al uso primario de los datos personales en el Reglamento del Espacio Europeo de Datos de Salud. Una visión panorámica», *Revista Jurídica de Castilla y León*, núm. 64, 2025, pp. 71-96.

DE MIGUEL BERIAIN, Íñigo./LÓPEZ DE LA PEÑA DE PABLO, Mercedes/LOYO-MENOYO, Mónica, «El nuevo reglamento europeo relativo al espacio europeo de datos de salud: su impacto en la gobernanza del dato y su uso ético y seguro», *Revista de Derecho y Genoma Humano*, núm. 61, 2025, pp. 1-30. DOI: https://doi.org/10.1387/rdgh.27342.

DE VERDA Y BEAMONTE, José Ramón, «Los derechos fundamentales de la personalidad (al honor, a la intimidad y a la propia imagen) como categoría unitaria», *Revista Boliviana de Derecho*, núm. 23, 2017, pp. 54-111.

DE LECUONA, Itziar, «Evaluación de los aspectos metodológicos, éticos, legales y sociales de proyectos de investigación en salud con datos masivos (big data)», *Gaceta Sanitaria*, vol. 32, núm. 6, 2018, pp. 576-578.

DÍEZ-PICAZO, Luis, *La doctrina de los propios actos*, Bosch, Barcelona, 1963.

DÍEZ-PICAZO, Luis y GULLÓN BALLESTEROS, Antonio, *Sistema de Derecho Civil*, vol. I, 12.ª ed., Tecnos, Madrid, 2012.

EVANGELIO LLORCA, Raquel, «Responsabilidad civil e inteligencia artificial en el ámbito sanitario», en Álvarez Lata, Natalia (coord.) *et al., Derecho de contratos, responsabilidad extracontractual e inteligencia artificia*l, Aranzadi, Cizur Menor, 2024, pp. 149-222.

GARCÍA RUBIO, María Paz, «Los derechos de la personalidad», en GETE-ALONSO Y CALERA, María del Carmen/SOLÉ RESINA, Judith (coords.), *Tratado de Derecho de la persona física*, Civitas-Thomson Reuters, Cizur Menor, 2013, pp. 595-631.

GONZÁLEZ FUSTER, Gloria, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Springer, Cham, 2014. DOI: https://doi.org/10.1007/978-3-319-05023-2.

GYMREK, Melissa, MCGUIRE, Amy Lynn L, GOLAN, DAVID, HALPERIN, ERAN, y ERLICH, Yaniv, «Identifying Personal Genomes by Surname Inference», *Science*, vol. 339, núm. 6117, 2013, pp. 321-324. https://doi.org/10.1126/science.1229566.

JORQUI AZOFRA, María, «DERECHOS Y DISPOSICIONES RELATIVAS AL USO PRIMARIO DE LOS DATOS DE SALUD ELECTRÓNICOS PERSONALES», EN EGUSQUIZA BALMASEDA, M.ª ÁNGELES/LUQUIN BERGARECHE, RAQUEL/JORQUI AZOFRA, MARÍA/VIDÁN PEÑA, JAVIER, *Régimen jurídico de protección de datos de salud en el Espacio Europeo de Datos de Salud (EEDS)*, Colex, A Coruña, 2025, pp. 49-114.

KOZIOL, Helmuth, «Punitive Damages: Admission into the Club?», *Journal of European Tort Law*, vol. 1, núm. 1, 2010, pp. 9-37. DOI: https://doi.org/10.1515/JETL.2010.9.

LAZCOZ MORATINOS, Guillermo, «La vigilancia o supervisión humana en el artículo 14 del Reglamento de inteligencia artificial: ¿un mero requisito obligatorio para los sistemas de alto riesgo?», en Cotino Hueso, Lorenzo/Simón Castellano, Pere (dirs.), *Tratado sobre el Reglamento de Inteligencia Artificial de la Unión Europea*, Aranzadi, Las Rozas, 2024, pp. 681-699.

LAZCOZ MORATINOS, Guillermo/DE MIGUEL BERIAIN, Íñigo, «Is more data always better? On alternative policies to mitigate bias in Artificial Intelligence health systems», *Bioethics*, vol. 39, núm. 5, 2025, pp. 414-424. DOI: https://doi.org/10.1111/bioe.13398.

LOZA CORERA, María, «Datos y gobernanza de datos y conexiones con principios protección de datos en el artículo 10 del Reglamento», en COTINO HUESO, LORENZO/SIMÓN CASTELLANO, PERE (DIRS.), *Tratado sobre el Reglamento de Inteligencia Artificial de la Unión Europea*, Aranzadi, Las Rozas, 2024, pp. 565-591.

LÓPEZ ULLA, Juan Manuel, «El acceso a los datos relativos a la salud: criterios aplicables de acuerdo con la Ley de transparencia y a la luz de la jurisprudencia del Tribunal Europeo de Derechos Humanos», *Papeles el tiempo de los derechos*, núm. 12, 2018, pp. 1-21.

MARTÍN JIMÉNEZ, Francisco Javier, «Big Data: riesgos y soluciones desde el Derecho y desde los principios», *Revista de Derecho Político*, núm. 119, 2024, pp. 215-249.

OHM, Paul, «Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization», *UCLA Law Review*, vol. 57, 2010, pp. 1701-1777.

NAVAS NAVARRO, Susana (Dir.), *Salud e inteligencia artificial desde el Derecho privado. Con especial atención a la pandemia por SARS-CoV-2 (covid-19),* Comares, Granada, 2021.

NAVAS NAVARRO, Susana, «Computación en la nube: Big Data y protección de datos personales», *InDret*, núm. 4, 2015, pp. 1-48.

NAVAS NAVARRO, Susana, «Neurodatos y Espacio Europeo de Datos de Salud. Los "intereses legítimos" del usuario de datos», *Cuadernos de Derecho Privado*, núm. 14, 2026, pp. 139-173. DOI: https://doi.org/10.62158/cdp.93.

NISSENBAUM, H., *Privacy in Context: Technology, Policy, and the Integrity of Social Life,* Stanford University Press, Stanford, 2010.

ORDÁS ALONSO, Marta, «Intimidad, secreto médico y protección de datos sanitarios», en GARCÍA AMADO, J. A. (coord.), *Razonar sobre derechos*, Tirant lo Blanch, Valencia, 2016, pp. 773-834.

PELLEGRINO, Edmun Daniel. y THOMASMA, David Charles, *A Philosophical Basis of Medical Practice*, Oxford University Press, New York, 1981.

PENASA, Simone, *et al.,* «The EU General Data Protection Regulation: How will it impact the regulation of research biobanks? Setting the legal frame in the Mediterranean and Eastern European area», *Medical Law International*, vol. 18, núm. 4, 2018, pp. 241-255. DOI: https://doi.org/10.1177/0968533218765044.

PERNA, Roberta, CRUZ-MARTÍNEZ, Gibrán y MORENO FUENTES, Francisco javier, «Movilidad de pacientes y descentralización sanitaria: respuestas y retos en el Sistema Nacional de Salud español», *Gestión y Análisis de Políticas Públicas*, núm. 30, 2022, pp. 27-44. https://doi.org/10.24965/gapp.i30.10978.

PÉREZ-UGENA, María, «La inteligencia artificial: definición, regulación y riesgos para los derechos fundamentales», Estudios de Deusto. Revista de Derecho Público, vol. 72, núm. 1, 2024, pp. 307-337. https://doi.org/10.18543/ed.3108.

PÉREZ DE LAS HERAS, Beatriz, «Hacia el Mercado Único Digital en la Unión Europea: retos y potencialidades para los entes subestatales», *Ekonomiaz*, núm. 98, 2020, pp. 150-171.

PRIETO SANCHÍS, Luis, «El constitucionalismo de los derechos», *Revista Española de Derecho Constitucional*, vol. 24, núm. 71, 2004, pp. 47-72. https://dialnet.unirioja.es/servlet/articulo?codigo=918875.

REBOLLO DELGADO, Lucrecio, El derecho fundamental a la protección de datos personales, Dykinson, Madrid, 2018.

RECUERO, Mikel, «El uso secundario de datos de salud electrónicos: el futuro Reglamento del Espacio Europeo de Datos de Salud y su interacción con la protección de datos personales», *InDret*, núm. 2, 2024, pp. 525-551. DOI: https://doi.org/10.31009/InDret.2024.i2.13.

ROCHER, Luc, HENDRICKX, Julien M. y DE MONTJOYE, Yves-Alexandre, «Estimating the Success of Re-identifications in Incomplete Datasets Using Generative Models», *Nature Communications*, vol. 10, 2019, art. 3069. https://doi.org/10.1038/s41467-019-10933-3.

RUBÍ PUIG, Antoni, «Daños por infracciones del derecho a la protección de datos personales. El remedio indemnizatorio del artículo 82 RGPD», *Revista de Derecho Civil*, vol. V, núm. 4, 2018, pp. 53-87.

RUBÍ PUIG, Antoni, «Espacio Europeo de Datos de Salud y responsabilidad civil. La norma indemnizatoria del artículo 100 del Reglamento (UE) 2025/327», en MORENO MARTÍNEZ, Juan Antonio (coord.), *Uso de Inteligencia Artificial en la Cirugía 4.0 y Salud Digital: Incidencias Jurídicas -Perspectivas Tecnológicas, Médicas y Legales-,* Dykinson, Madrid, 2026, pp. 877-928.

SÁIZ RAMOS, Macarena/LARIOS RISCO, David, «El derecho de acceso a la historia clínica por el paciente: propuesta para la reserva de anotaciones subjetivas», *Derecho y Salud*, vol. 18, núm. 1, 2009, pp. 21-41.

SÁNCHEZ GÓMEZ, Amelia, «Las nuevas tecnologías y su impacto en los derechos al honor, intimidad, imagen y protección de datos del menor. Mecanismos jurídicos de protección: carencias, interrogantes y retos del legislador», *Revista Boliviana de Derecho*, núm. 23, 2017, pp. 168-191.

SIMÓN MARCO, Jesús María, «Evolución del derecho a la protección de datos y disrupción tecnológica: ¿estamos vallando el campo?», *Revista CEFLegal*, núm. 233, 2020, pp. 89-120.

SHRINGARPURE, Suyash S., y BUSTAMANTE, Carlos Daniel, «Privacy Risks from Genomic Data-Sharing Beacons», *American Journal of Human Genetics*, vol. 97, núm. 5, 2015, pp. 631-646. https://doi.org/10.1016/j.ajhg.2015.09.010.

WACHTER, Sandra y MITTELSTADT, Brent, «A right to reasonable inferences: re-thinking data protection law in the age of big data and AI», *Columbia Business Law Review*, vol. 2019, núm. 2, 2019, pp. 494-620. Disponible en: https://doi.org/10.7916/cblr.v2019i2.3424.

ZECH, Herbert, «A legal framework for a data economy in the European Digital Single Market: rights in data», *Journal of Intellectual Property Law & Practice*, vol. 11, núm. 6, 2016, pp. 460-470. DOI: https://doi.org/10.1093/jiplp/jpw072.

VILLANUEVA TURNES, Alejandro, «El derecho a la intimidad y el consentimiento de los menores de edad. Especial referencia a las redes sociales», *Revista Boliviana de Derecho*, núm. 23, 2017, pp. 208-221.