BAIDATA

INTERNATIONAL DATA SPACES ASSOCIATION

Determinación de la responsabilidad por vulneraciones de datos en el intercambio de datos entre varias partes conforme al marco regulatorio de la UE

Traducción del informe "Allocation of liability for data breaches in multi-party data sharing under EU regulatory frameworks" de la iniciativa DSSC

DATA SPACES SUPPORT CENTRE

Título del Documento: Determinación de la responsabilidad por violaciones de datos en el intercambio de datos entre varias partes conforme al marco regulatorio de la UE.

Subtítulo: Traducción del informe "*Allocation of liability for data breaches in multi-party data sharing under EU regulatory frameworks*" de la iniciativa DSSC

Versión: 1.0

Fecha de Publicación: marzo de 2026

Publicado por: BAIDATA

Descargo de Responsabilidad: El contenido de este documento se fundamenta en el documento *Allocation of liability for data breaches in multi-party data sharing under EU regulatory frameworks* la iniciativa DSSC.

Tabla de contenido

FICHA TÉCNICA

¿Qué es este documento?

El documento es un informe del Data Spaces Support Centre que analiza la responsabilidad legal ante la vulnerabilidad de datos en los espacios de datos europeos, especialmente bajo el marco de RGPD, NIS2 y la Ley de Gobernanza de Datos.

¿Qué encontraré en este documento?

El informe ofrece un análisis de quién es responsable legalmente ante una vulnerabilidad de datos en un espacio de datos, y cómo encajan el RGPD, NIS2 y la Ley de Gobernanza de Datos en esa responsabilidad. También explica las obligaciones de notificación, documentación y gestión del riesgo que surgen cuando ocurre un incidente de seguridad.

¿Por qué y para quién es interesante este documento?

Este documento resulta de gran interés para los miembros y socios de ecosistemas de datos, en particular aquellos vinculados a empresas, proveedores de servicios, departamentos legales y profesionales de ciberseguridad, ya que les ayuda a entender sus obligaciones bajo el RGPD, cómo gestionar riesgos legales y qué medidas adoptar para proteger los datos y reducir responsabilidades. Este documento resulta interesante porque analiza cómo se asigna la responsabilidad legal frente a brechas de datos, especialmente en entornos colaborativos como los espacios de datos.

Recuerde que este documento es una traducción del informe original publicado por el proyecto DSSC *"Allocation of liability for data breaches in multi-party data sharing under EU regulatory frameworks"*. Puede consultar el documento original en este enlace.

RESUMEN EJECUTIVO

El presente documento es una traducción al español realizada por BAIDATA de un informe de referencia del Data Spaces Support Centre (DSSC). El informe **"Legal Liability for Data Breaches"** de la **DSSC** analiza cómo se determina la responsabilidad jurídica en caso de vulneraciones de datos dentro del marco europeo, destacando que no es automática ni recae en un único actor, sino que depende de varios factores como el cumplimiento del RGPD, la adopción de medidas técnicas y organizativas adecuadas y la existencia de una relación causal entre el fallo de seguridad y el daño producido.

La responsabilidad varía según el rol de los participantes (principalmente responsables y encargados del tratamiento) y, en entornos complejos como los espacios de datos, suele ser compartida entre múltiples entidades, lo que hace imprescindible definir claramente en contratos las funciones, obligaciones y reparto de riesgos. El informe también subraya que pueden derivarse distintas consecuencias legales, incluyendo sanciones administrativas, responsabilidad civil con indemnizaciones por daños materiales e inmateriales, y responsabilidad contractual entre las partes.

En este contexto, la clave no es solo evitar brechas, sino demostrar diligencia y cumplimiento mediante una gobernanza sólida, medidas de ciberseguridad eficaces, documentación adecuada y mecanismos claros de gestión y notificación de incidentes, en un entorno donde la complejidad jurídica y tecnológica sigue en aumento.

1 INTRODUCCIÓN

Los riesgos para la privacidad y la seguridad asociados al intercambio de datos confidenciales, así como los incidentes accidentales y así como la creciente frecuencia de incidentes de ciberseguridad[1], tanto intencionales como accidentales, pueden hacer que las organizaciones y las individuos se muestren reacios a participar en espacios de datos. Estas preocupaciones se acentúan aún más en entornos federados y transfronterizos, donde la fragmentación de las regulaciones y la falta de claridad en los marcos de responsabilidad generan una mayor incertidumbre jurídica.

Esto pone de relieve la necesidad de contar con marcos de responsabilidad claros y exigibles para los espacios de datos. En particular, en sectores de alta sensibilidad, como la salud y las finanzas, todos los participantes en los espacios de datos deben poder demostrar el cumplimiento de las obligaciones aplicables en materia de seguridad y protección de datos, así como la clara asignación [2]de responsabilidades ante posibles incidentes. Para lograrlo, los participantes deben definir sus respectivas funciones y obligaciones en una forma adecuada y proporcional a los riesgos identificados.

El marco normativo que regula la seguridad del intercambio de datos es multidimensional[3] e incluye:

- Marcos normativos fundamentales para la ciberseguridad, como la Directiva sobre redes y sistemas de información (NIS2) [4]y la Ley de Ciberresiliencia (CRA).[5]

[1] Los incidentes de ciberseguridad pueden producirse de forma intencionada o accidental. La ciberseguridad se refiere a «la organización y el conjunto de recursos, procesos y estructuras utilizados para proteger el ciberespacio y los sistemas que operan en él frente a situaciones en las que los derechos de propiedad de jure no se ajustan a los de facto»; es decir, protege una serie de activos entre los que se incluyen la información, las personas y sus intereses, frente a amenazas que puedan aprovechar vulnerabilidades o que surjan a causa del sistema TIC o de la propia información. Véase, por ejemplo, Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. Technology Innovation Management Review, 4(10).

[2] ENISA (2024). Engineering Personal Data Protection in EU Data Spaces v1.0. https://www.enisa.europa.eu/sites/default/files/publications/Data%20Spaces%20Report.pdf

[3]Ver también, ENISA(2023) Multilayer framework for good cybersecurity practices for AI. https://www.enisa.europa.eu/publications/multilayer-framework-for-good-cybersecurity-practicesfor-ai

[4] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive) http://data.europa.eu/eli/dir/2022/2555/2022-12-27

[5] Reglamento (UE) 2024/2847 del Parlamento Europeo y del Consejo de 23 de octubre de 2024 relativo a los requisitos horizontales de ciberseguridad para los productos con elementos digitales (Reglamento de Ciberresiliencia). https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=OJ:L_202402847

- Marcos normativos específicos para el intercambio de datos, como el Reglamento General de Protección de Datos (RGPD), la Ley de Gobernanza de Datos (DGA) y la Ley de Datos.
- Normativas específicas de cada sector, como la Ley de Resiliencia Operativa Digital (DORA) [6]y el Reglamento sobre el Espacio Europeo de Datos Sanitarios (EHDS).[7]

La implementación de estas normas viene determinada por las características estructurales, operativas, regionales y sectoriales de cada espacio de datos. Esta variabilidad dificulta el desarrollo de marcos jurídicos uniformes para un espacio de datos, especialmente en sectores como la sanidad, las finanzas y la energía, en los que se aplican requisitos estrictos a la protección de datos sensibles e infraestructuras críticas[8].

En cualquier caso, la legislación en materia de ciberseguridad y las responsabilidades asociadas siguen sin haberse analizado en profundidad en el contexto de los espacios de datos. Sin normas claras sobre cómo se distribuye la responsabilidad, los espacios de datos europeos corren el riesgo de volverse menos resistentes a las alteraciones, mientras que las organizaciones siguen mostrándose reacias a compartir sus datos debido a la incertidumbre jurídica. Para abordar esta laguna, este informe examina los marcos normativos clave para salvaguardar el intercambio de datos, entre ellos la NIS2, el RGPD y la DGA, cómo abordan la responsabilidad y su interacción, especialmente cuando varias entidades contribuyen al tratamiento y almacenamiento de datos. La evaluación describe en primera instancia las estructuras de responsabilidad establecidas por cada marco y, a continuación, ilustra sus limitaciones prácticas a través de dos ejemplos.

[6] Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 sobre la resiliencia operativa digital del sector financiero. https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32022R2554
[7] Reglamento (UE) 2025/327 del Parlamento Europeo y del Consejo de 11 de febrero de 2025 relativo al Espacio Europeo de Datos de Salud https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=OJ:L_202500327
[8] D. Sargiotis (2024). Legal and Regulatory Considerations in Data Governance. Data Governance. Springer, pp 445–466. https://doi.org/10.1007/978-3-031-67268-2_15

2 RESPONSABILIDADES LEGALES Y OPERATIVAS EN VIRTUD DE LA DIRECTIVA NIS2, EL RGPD Y LA DGA

2.1 NIS2: Responsabilidad en la gestión de los riesgos de ciberseguridad

La Directiva NIS2 establece obligaciones en materia de gestión de riesgos, notificación de incidentes y responsabilidades de gobernanza para las entidades «esenciales» e «importantes» que operan en 18 sectores críticos de toda la UE[9]. Para los espacios de datos que operan en los sectores incluidos en su ámbito de aplicación, como las infraestructuras y los servicios digitales, la sanidad, la industria manufacturera, la energía, el transporte, la banca y la administración pública, es fundamental cumplir los requisitos de la Directiva NIS2. La Directiva se basa en su predecesora, la NIS1, ampliando su ámbito de aplicación, introduciendo obligaciones más detalladas, aumentando la responsabilidad por incumplimiento y otorgando mayores poderes de supervisión y ejecución a los organismos reguladores nacionales. Si bien la NIS2 refuerza la armonización de la legislación en materia de ciberseguridad entre los Estados miembros, persisten las divergencias nacionales, ya que se trata de una directiva y está sujeta a la aplicación local. Cabe destacar que el alcance y la cobertura sectorial, los requisitos de auditoría, los requisitos de notificación de incidentes y la aplicación de la responsabilidad de los directivos varían de una jurisdicción a otra. Incluso las definiciones de entidades «esenciales» e «importantes» sujetas a la Directiva NIS2 difieren entre los Estados miembros, ya que algunos incluyen sectores adicionales más allá de los establecidos en la Directiva NIS2.[10]

[9] Véanse el artículo 3, el anexo I y el anexo II de la Directiva NIS2. Las entidades esenciales a efectos de la Directiva NIS2 incluyen a las grandes y medianas empresas de sectores críticos, entre los que se encuentran la energía, el transporte, las finanzas, la sanidad, el agua potable, las aguas residuales, las infraestructuras digitales, la gestión de servicios de TIC, la administración pública y el sector espacial. Asimismo, establece obligaciones para otras entidades importantes, enumeradas en el anexo II, como los servicios postales, las organizaciones de investigación y los fabricantes de productos sanitarios.

[10] Por ejemplo, Italia y Croacia incluyen a las instituciones educativas como sectores críticos en sus leyes nacionales de ciberseguridad. Decreto Legislativo No 138. Gazzetta Ufficiale Della Repubblica Italiana. Septiembre 2024. https://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.dataPubblicazioneGazzetta=2024-10-01&atto.codiceRedazionale=24G00155 y Uredbu o Kibernetičkoj Sigurnosti. NN 135/2024. https://narodne-novine.nn.hr/eli/sluzbeni/2024/135/2217

En virtud de la Directiva NIS2, las entidades esenciales e importantes están obligadas a aplicar medidas técnicas, operativas y organizativas adecuadas y proporcionadas para gestionar los riesgos de ciberseguridad. Estas medidas abarcan una serie de prácticas, entre las que se incluyen políticas de análisis y gestión de riesgos, procedimientos de gestión de incidentes, gestión de copias de seguridad y restauración ante desastres, seguridad de la cadena de suministro, criptografía y control de acceso (artículo 21, apartado 2, de la Directiva NIS2). Por ejemplo, las infraestructuras de intercambio de datos que operan en sectores sujetos a la Directiva NIS2 deben contar con mecanismos de autenticación seguros para garantizar que solo los usuarios autorizados puedan acceder a los datos. Cuando proceda, las entidades afectadas también deben implementar procedimientos de cifrado para proteger los datos durante su tratamiento, transmisión y almacenamiento.[11] Por suerte, el cumplimiento de normas de ciberseguridad reconocidas internacionalmente, como la norma ISO 27001 y la serie IEC 62443, puede facilitar notablemente el cumplimiento normativo.

En caso de que se produzca un incidente grave[12], las entidades afectadas están obligadas a notificarlo al equipo nacional de respuesta a incidentes de seguridad informática (CSIRT[13]). Si es posible que el incidente afecte negativamente a la prestación de sus servicios, también se deberá informar a los usuarios afectados. El artículo 23 define una estructura de notificación de incidentes por niveles. Las entidades esenciales e importantes deberán presentar una alerta preliminar en un plazo de 24 horas desde que tengan conocimiento del incidente, incluyendo una evaluación provisional de su causa y de su posible impacto transfronterizo.

En un plazo de 72 horas, debe enviarse una notificación más detallada en la que se describan la gravedad, el alcance y las posibles consecuencias del incidente. A continuación, se exige un informe final exhaustivo en el plazo de un mes. Aunque la NIS2 establece una serie de requisitos mínimos estrictos para la notificación de incidentes, los Estados miembros difieren en sus definiciones de lo que constituye un incidente significativo, el contenido obligatorio de los informes y los plazos de notificación[14]. Por ejemplo, Polonia y Eslovaquia ofrecen modelos de clasificación adicionales para los incidentes en función de su gravedad, y la adaptación de

[11] Las organizaciones pueden recurrir a técnicas punteras, como la computación confidencial, para minimizar la exposición de los datos sensibles y los flujos de ejecución de los programas.
[12] En virtud de la Directiva NIS2, un incidente se considera significativo si: (a) ha causado o puede causar una grave interrupción operativa de los servicios o pérdidas económicas para la entidad afectada; o (b) ha afectado o puede afectar a otras personas físicas o jurídicas causando daños materiales o inmateriales considerables (artículo 23, apartado 3, de la Directiva NIS2).
[13] Computer Security Incident Responde Team (CSIRT) – Equipo de Respuesta ante Incidencias de Seguridad Informática
[14] ECSO, (2025). White Paper: NIS2 Implementation challenges and priorities. Disponible en: https://ecsorg.eu/ecso-uploads/2025/01/ECSO-NIS2-White-Paper.pdf

la Directiva por parte de Chipre exige una notificación inicial en un plazo de seis horas desde su detección[15].

La asignación de responsabilidades en materia de cumplimiento de la Directiva NIS2 dentro de un espacio de datos depende en gran medida de la estructura organizativa adoptada para la infraestructura de intercambio de datos[16]. La Directiva NIS2 exige la participación activa de la cúpula directiva en la gobernanza de la ciberseguridad, requiriendo que apruebe y supervise la aplicación de las medidas de gestión de riesgos y de notificación (artículo 20 de la Directiva NIS2). Cada participante suele tener su propio comité de dirección, responsable de adoptar las medidas de seguridad adecuadas para gestionar los riesgos relacionados con el gobierno corporativo y la ciberseguridad. En algunos casos, el propio espacio de datos también puede constituirse como una entidad jurídica con su propio órgano directivo. Por ejemplo, una alianza estratégica basada en acuerdos contractuales entre participantes independientes presenta una estructura de responsabilidad diferente a la de una asociación, como Catena-X[17], que cuenta con su propio consejo ejecutivo encargado de la gobernanza y el cumplimiento normativo. Sin embargo, la NIS2 no define la responsabilidad en situaciones en las que interviene una infraestructura compartida a la que contribuyen varias entidades. Carece de un marco para atribuir responsabilidades cuando se producen incidentes derivados de infraestructuras compartidas e interdependientes gestionadas por varias organizaciones.

En caso de incumplimiento, la Directiva NIS 2 conlleva importantes repercusiones, entre las que se incluyen sanciones tanto de carácter monetario como no, y amplía la responsabilidad jurídica a los representantes a título individual. Los miembros del órgano de dirección pueden ser considerados personalmente responsables en caso de que no garanticen el cumplimiento de las obligaciones en materia de ciberseguridad[18]. En función de la aplicación nacional, las autoridades reguladoras pueden imponer multas y solicitar la suspensión de miembros concretos del consejo de administración en caso de incumplimiento. Además, las infracciones pueden dar lugar a importantes multas administrativas para las entidades en

[15] ECSO, (2025). White Paper: NIS2 Implementaiton challenges and priorities. Disponible en: https://ecsorg.eu/ecso-uploads/2025/01/ECSO-NIS2-White-Paper.pdf

[16] Ver más: Plan de DSSC v3.0: Estructura organizativa y autoridad de gobernanza. https://blueprint.dssc.eu/?pane=business&business=organisational-form-and-governance-authority

[17] El comité ejecutivo de Catena-X está compuesto por 12 miembros que representan a diferentes organizaciones, como BMW, Siemens, el Grupo Renault, SAP y Fraunhofer ISST. Más información en https://catena-x.net/association/structureand-role/

[18] Ver artículo 32 apartado 5 y 6 del NIS2

cuestión[19]. Las autoridades nacionales de supervisión también pueden imponer sanciones no económicas, como advertencias, órdenes vinculantes y obligaciones de cumplimiento.[20] Sin embargo, el alcance y el efecto de las sanciones no económicas se limitan a la jurisdicción de la autoridad que las impone y no se aplican en todos los Estados miembros.

2.2 RGPD: Responsabilidad en materia de protección de datos personales

El RGPD establece principios fundamentales para el tratamiento de datos personales, como la delimitación de la finalidad, la minimización de datos y la responsabilidad.[21] Estos principios tienen repercusiones directas en la gobernanza de la ciberseguridad dentro de las organizaciones que tratan datos personales, ya que refuerzan las prácticas de gestión de datos responsables y conscientes de los riesgos en toda la UE. En este sentido, el reglamento actúa tanto como facilitador como delimitador para el intercambio seguro de datos. Por un lado, refuerza los derechos de los usuarios sobre los datos, mejora la transparencia entre los participantes en el espacio de datos y fomenta técnicas de análisis de datos que protegen la privacidad, como el aprendizaje federado y la gestión descentralizada de datos, lo que aumenta la confianza en el intercambio de datos.[22] Por otro lado, la asignación de funciones y responsabilidades en virtud del RGPD puede resultar excesivamente compleja en ecosistemas de datos dinámicos y con múltiples actores, lo que puede dar lugar a ineficiencias operativas.

La designación clara de los responsables del tratamiento del dato (*data controller*)[23], los corresponsables[24] y los encargados del tratamiento (*data processor*)[25], junto con una definición clara de sus respectivos roles y responsabilidades en virtud del RGPD, es esencial para establecer una gobernanza operativa eficaz en el contexto de los espacios de datos. Los

[19] En virtud del artículo 34, las entidades esenciales pueden ser sancionadas con multas de hasta 10 millones de euros o el 2 % de su volumen de negocios anual a nivel mundial, el que sea mayor. Las entidades importantes pueden enfrentarse a sanciones económicas de hasta 7 millones de euros o el 1,4 % de su volumen de negocios anual a nivel mundial.

[20] Ver artículos 32(4) y 33(4), del NIS2

[21] Consulte la lista completa y las descripciones de los principios recogidos en el artículo 5, apartado 1, del RGPD

[22] Vukovic, J., Ivankovic, D., Habl, C., Dimnjakovic, J., (2022). Enablers and barriers to the secondary use of health data in Europe: general data protection regulation perspective. Arch Public Health, 80(1):115, doi: 10.1186/s13690-022-00866-7

[23] Un responsable del tratamiento es la entidad que decide determinados aspectos fundamentales del procesamiento. La condición de responsable del tratamiento puede estar definida por ley o derivarse de un análisis de los hechos o circunstancias del caso. Véanse, por ejemplo, el artículo 4, apartado 7, y el artículo 24 del RGPD.

[24] En el caso de la responsabilidad conjunta, dos o más entidades determinan los fines y los medios del tratamiento.

[25] Según el artículo 4, apartado 8, del RGPD, se entiende por «encargado del tratamiento» toda persona física o jurídica, autoridad pública, agencia u otro organismo que trate datos personales por cuenta del responsable del tratamiento.

responsables del tratamiento son quienes deben aplicar las medidas técnicas y organizativas adecuadas para garantizar el cumplimiento de los principios, velar por los derechos de los interesados, asegurar la seguridad de las operaciones de tratamiento, mantener registros de incidentes y realizar evaluaciones de impacto relativas a la protección de datos (EIPD) cuando el tratamiento pueda suponer un riesgo elevado para los derechos y libertades de las personas.[26] La selección y evaluación de las medidas deben adaptarse al contexto concreto, teniendo en cuenta la naturaleza, el alcance, la finalidad y los riesgos asociados al procesamiento, así como el posible impacto en los derechos de los interesados afectados por dicho procesamiento.[27]

El RGPD exige que los responsables y los encargados del tratamiento formalicen un contrato jurídicamente vinculante en el que se definan el objeto y la duración del tratamiento, la naturaleza y la finalidad del mismo, el tipo de datos personales y las categorías de interesados, así como las obligaciones y derechos respectivos de las partes (artículo 28, apartado 3, del RGPD). Los responsables y los encargados del tratamiento deben garantizar que los acuerdos de tratamiento de datos definan claramente el alcance de las responsabilidades del encargado y establezcan mecanismos para la resolución de litigios y la atribución de responsabilidad, en particular en relación con las reclamaciones de indemnización. Además, en el caso de infraestructuras compartidas, las partes deben acordar notificar a otros responsables o encargados del tratamiento que participen en la misma actividad de tratamiento cualquier incumplimiento relevante, queja o reclamación recibida de los interesados.

Sin embargo, las distinciones entre responsables del tratamiento, responsables conjuntos y encargados del tratamiento, así como las obligaciones asociadas a cada una de estas funciones, no siempre encajan a la perfección con los modelos de gobernanza previstos en los espacios de datos. Las funciones son de carácter funcional, lo que significa que su asignación viene determinada por las actividades reales en un contexto específico y, por lo tanto, suele derivarse de un análisis de las circunstancias concretas de cada caso, más que de una designación contractual.[28] La naturaleza de la actividad de tratamiento y el grado de

[26] Véase el artículo 32 sobre la seguridad del tratamiento, el artículo 5, apartado 2, sobre los principios relativos al tratamiento, los artículos 24 y 25 sobre las obligaciones generales, y el artículo 35 sobre las evaluaciones de impacto relativas a la protección de datos.
[27] AEPD (2023), «Enfoque de los espacios de datos desde la perspectiva del RGPD», p. 35
[28] EDPB (2021) Directrices 07/2020 sobre los conceptos de responsable del tratamiento y encargado del tratamiento en el RGPD, versión 2.1. https://www.edpb.europa.eu/system/files/2023-10/EDPB_guidelines_202007_controllerprocessor_final_en.pdf

influencia sobre los fines y los medios del tratamiento afectan a la delimitación de las funciones y determinan cómo se asignan las responsabilidades.

Los responsables del tratamiento son responsables de cualquier daño material o moral derivado del incumplimiento, incluidos los derivados de ciberataques de terceros, si no logran demostrar que han aplicado las medidas técnicas y organizativas adecuadas.[29] Además de las vulnerabilidades derivadas de sus propios sistemas, un responsable del tratamiento también puede sufrir una violación de la seguridad de los datos personales que afecten a datos tratados en su nombre por un encargado del tratamiento. Por lo general, los encargados del tratamiento no son directamente responsables de las infracciones, siempre que sus actividades de tratamiento no excedan ni contradigan las instrucciones del responsable del tratamiento. No obstante, en determinados casos, los encargados del tratamiento pueden incurrir en responsabilidad directa por el incumplimiento de las obligaciones que les impone específicamente el RGPD, como la falta de aplicación de medidas técnicas y organizativas adecuadas para garantizar un tratamiento seguro.[30] Las autoridades de control pueden imponer sanciones administrativas tanto a los responsables del tratamiento como a los encargados del tratamiento, incluidas multas y prohibiciones temporales o definitivas del tratamiento de datos.[31]

2.3 DGA: Responsabilidad frente a garantías óptimas

El Reglamento de Gobernanza de Datos (DGA) establece medidas de protección para fomentar el intercambio de datos tanto personales como no personales sujetos a protecciones legales, entre las que se incluyen la confidencialidad comercial, la confidencialidad estadística, los derechos de propiedad intelectual y la privacidad. Estas salvaguardias incluyen: la definición de las condiciones de reutilización de los datos

[29] El artículo 82 del RGPD establece el derecho a indemnización de las personas que sufran daños materiales o morales causados por infracciones.
[30] Véase, por ejemplo, la resolución administrativa del presidente polaco de la Oficina de Protección de Datos Personales por la que se impone una multa al encargado del tratamiento por no haber prestado asistencia al responsable del tratamiento en la aplicación de las medidas de seguridad técnicas y organizativas adecuadas (incumplimiento del artículo 32 del RGPD). Disponible en: https://uodo.gov.pl/decyzje/DKN.5131.1.2021 (resolución en polaco) y resumen del Comité Europeo de Protección de Datos https://www.edpb.europa.eu/news/national-news/2025/polish-sa-administrative-fine-81-000-eu-failure-implement-appropriate_en
[31] Véase el artículo 83 sobre las condiciones generales para la imposición de sanciones administrativas. Las sanciones por la mayoría de las infracciones ascienden a un máximo de 10 millones de euros o al 2 % de la facturación anual mundial, el importe que sea mayor, mientras que las infracciones graves pueden acarrear sanciones de hasta 20 millones de euros o el 4 % de la facturación global.

protegidos en poder de los organismos del sector público, la implementación de espacios federados seguros (*SPE* siglas en inglés) para las categorías de datos sensibles, y los requisitos y la supervisión de los Proveedores de Servicios de Intermediación de Datos (PSID) y las organizaciones de altruismo de datos (*DAO* siglas en inglés).

El artículo 5 de la DGA habilita a los organismos del sector público a permitir la reutilización de datos protegidos y describe dos técnicas para garantizar una seguridad adecuada. Los organismos del sector público pueden, bien aplicar métodos que preserven la privacidad y la confidencialidad —como la anonimización y la simplificación— para facilitar el acceso a los datos, bien poner los datos a disposición en el marco de los entornos de protección de datos (SPE). La DGA recomienda el uso «óptimo» de métodos de preservación de la privacidad, animando a los organismos del sector público a poner a disposición la mayor cantidad de datos posible (Considerando 7, DGA). Sin embargo, la determinación de los niveles adecuados de protección y de los requisitos y especificaciones técnicas de los SPE se deja en manos de los organismos del sector público y de la interpretación a nivel sectorial.

En el caso de los PSID, la DGA impone varios requisitos de seguridad para el acceso a los datos. En virtud del artículo 12, los PSID deben implementar las medidas de seguridad técnicas, jurídicas y organizativas adecuadas para impedir el acceso o la transferencia ilícitos de datos no personales (j) y mantener un nivel adecuado de seguridad para el almacenamiento, el tratamiento y la transmisión de dichos datos (l). Teniendo en cuenta la diferente naturaleza de los datos, el DGA exige además «el más alto nivel de seguridad» para el almacenamiento y la transmisión de información sensible desde el punto de vista de la competencia. Del mismo modo, las DAO están obligadas a mantener un nivel adecuado de seguridad para el almacenamiento y el tratamiento de datos no personales (artículo 21, apartado 4, de la DGA).

En caso de transferencia, acceso o uso no autorizados de datos no personales, tanto los PSID como los DAO están obligados a notificarlo sin demora injustificada a los titulares de los datos correspondientes.[32] Del mismo modo, en caso de reutilización no autorizada de datos no personales procedentes de un organismo del sector público, el reutilizador de los datos tiene

[32] Por «titular de los datos» se entiende una persona jurídica, incluidos los organismos del sector público y las organizaciones internacionales, o una persona física que no sea el interesado en relación con los datos específicos de que se trate, la cual, de conformidad con el Derecho de la Unión o el Derecho nacional aplicable, tiene derecho a conceder acceso a determinados datos personales o datos no personales, o a compartirlos (artículo 2, apartado 8, de la DGA).

la responsabilidad de informar a las personas jurídicas cuyos derechos o intereses puedan verse perjudicados (artículo 5, apartado 5, de la DGA).

Por lo demás, la responsabilidad y las sanciones previstas en la DGA dependen de la aplicación pública por parte de las autoridades nacionales competentes, lo que deja un margen considerable para la fragilidad normativa. Las autoridades nacionales tienen la tarea de definir y aplicar sanciones efectivas, proporcionadas y preventivas en sus respectivos marcos jurídicos (artículo 34 de la DGA). Asimismo, dependiendo de los marcos jurídicos nacionales aplicables y de los términos de los acuerdos contractuales, los titulares de los datos y los usuarios de los datos pueden recurrir a vías de ejecución privadas, tales como acciones por cumplimiento contractual, reclamaciones por daños y perjuicios, terminación del acuerdo o solicitudes de medidas cautelares.

En los casos relacionados con datos personales, la DGA se rige por el RGPD. Los titulares de los datos son responsables de garantizar la recopilación, el tratamiento y el almacenamiento legales de los datos personales, mientras que los PSID actúan como facilitadores, permitiendo el intercambio, el tratamiento y el acceso controlados a los datos. Las entidades que determinan los fines y los medios del tratamiento asumen el papel de responsables del tratamiento en virtud del RGPD. Sin embargo, identificar a los responsables y a los encargados del tratamiento en la práctica puede resultar complejo, ya que depende de la estructura específica y de los acuerdos contractuales que rigen la operación de intercambio de datos.

3 LAS VULNERACIONES DE DATOS Y LA ATRIBUCIÓN DE RESPONSABILIDAD EN LOS ESPACIOS DE DATOS

3.1 Ejemplo 1: Vulneraciones de datos en infraestructuras federadas de intercambio de datos

Las infraestructuras federadas representan un enfoque descentralizado para el intercambio de datos que permite a los titulares de los datos mantener el control sobre estos, ya que los datos permanecen dentro de sus entornos seguros. Este enfoque reduce la necesidad de duplicar datos y ayuda a evitar las restricciones normativas que suelen asociarse a los sistemas centralizados. Estas infraestructuras pueden utilizarse para entrenar modelos algorítmicos de forma descentralizada sin transferir datos, una técnica conocida como *aprendizaje federado*.

El aprendizaje federado se considera generalmente un enfoque que mejora la protección de la privacidad.[33] En el aprendizaje federado, los modelos algorítmicos se entrenan localmente en las instalaciones de los titulares de los datos, y solo los parámetros entrenados o las actualizaciones del modelo se comparten y se agregan en un servidor central de coordinación. Una vulnerabilidad en el servidor central o en un solo titular de datos puede comprometer la integridad del modelo global, lo que afectaría a varios participantes. Si bien cada titular de datos es responsable de garantizar la calidad de los datos y la seguridad local, el servicio de coordinación asume la responsabilidad de agregar y distribuir el modelo global.

Este modelo se contempla, por ejemplo, en el proyecto de la Federación Europea de Imágenes Oncológicas (EUCAIM)[34] para el desarrollo de algoritmos de imágenes oncológicas. En la estructura de aprendizaje federado de EUCAIM, el software de EUCAIM tiene acceso a los almacenes de datos locales de los hospitales, que cumplirán las normas y los requisitos de seguridad y calidad definidos por EUCAIM. Los titulares de datos que participan en EUCAIM

[33] Ver: Xu, J., Glicksberg, B.S., Su, C. et al. Federated Learning for Healthcare Informatics. J Healthc Inform Res 5, 1–19 (2021). https://doi.org/10.1007/s41666-020-00082-4
[34] https://cancerimage.eu/

son entidades esenciales en virtud de la NIS2 y tratan datos altamente sensibles en virtud del RGPD. Si bien el aprendizaje federado reduce los riesgos relacionados con la privacidad y ayuda a los hospitales a cumplir con el RGPD, presenta una infraestructura compartida e interdependiente gestionada por múltiples organizaciones, lo que complica la asignación de la responsabilidad.

Las vulnerabilidades en los sistemas locales de los hospitales o en el servidor central de coordinación pueden comprometer la integridad de los datos, propagar actualizaciones de modelos corruptos y afectar a la precisión del diagnóstico en todos los centros participantes. Por ejemplo, si el almacén de datos local de un hospital se ve comprometido por un ataque de *ransomware* (software malicioso) o por una vulnerabilidad en la cadena de suministro durante el proceso de extracción de la historia clínica electrónica (HCE), podrían introducirse datos corruptos en el proceso de aprendizaje federado. Aunque los datos nunca salgan de las instalaciones del hospital, la integración de datos comprometida en un solo nodo puede propagarse a través del proceso de aprendizaje federado, afectar de manera crítica al modelo global de IA y manipular las predicciones de diagnóstico de cáncer en todos los centros participantes. Esto aumenta la complejidad a la hora de asignar la responsabilidad entre el titular de los datos que introdujo la vulnerabilidad, el servicio de coordinación que gestiona el modelo global y los usuarios de los datos que confían en los resultados comprometidos. Todos estos actores asumen responsabilidades en virtud de las transposiciones nacionales de la NIS2, así como de las leyes nacionales, frente a los pacientes individuales que puedan verse afectados. La ausencia de normas armonizadas sobre la responsabilidad interorganizacional genera una importante incertidumbre jurídica.

Otro ámbito operativo que se vuelve especialmente complejo en tales situaciones es la responsabilidad de la notificación obligatoria de incidentes con arreglo a la Directiva NIS2. Ya pueden surgir dificultades a la hora de evaluar qué constituye un incidente significativo. Según la Directiva NIS2, no es necesario que un incidente provoque una grave interrupción operativa o pérdidas económicas para que se considere significativo; basta con que exista la mera capacidad de causar tales daños.[35] Además, las autoridades nacionales pueden tener interpretaciones divergentes de este umbral, lo que da lugar a incoherencias entre los Estados miembros. Si un único hospital o el servicio de coordinación sufre un incidente significativo

[35] De conformidad con el artículo 23, apartado 3, de la Directiva NIS2, un incidente se considera significativo si: a) ha causado o puede causar una grave interrupción operativa de los servicios o pérdidas económicas para la entidad afectada; o b) ha afectado o puede afectar a otras personas físicas o jurídicas causando daños materiales o inmateriales considerables.

que afecte o pueda afectar negativamente a la infraestructura EUCAIM, los participantes tendrán que evaluar sus obligaciones de notificación caso por caso y coordinarse en consecuencia.

La coordinación cobra aún mayor importancia si el incidente da lugar a la obligación de notificarlo a varias autoridades nacionales, ya que los estrictos plazos y requisitos de notificación establecidos en la Directiva NIS2 y el RGPD pueden variar considerablemente de una jurisdicción a otra. Por consiguiente, es fundamental que EUCAIM y otras infraestructuras federadas de intercambio de datos cuenten con procesos predefinidos que garanticen una notificación oportuna, precisa y conforme a la normativa a todas las autoridades pertinentes.

3.2 Ejemplo 2: Asignación de responsabilidad en entornos de procesamiento seguros

En virtud de la DGA, los organismos públicos pueden exigir que la reutilización de datos protegidos se lleve a cabo en espacios federados seguros (SPE) (Artículo 5, apartado 3, de la DGA). Si bien los SPE son un concepto emergente en la legislación de la UE y su aplicación práctica varía, su objetivo es proporcionar un entorno controlado para el acceso y el tratamiento de datos sensibles. La DGA los describe como entornos físicos o virtuales combinados con medidas organizativas que garantizan el cumplimiento de la legislación de la UE y permiten al proveedor del SPE determinar y supervisar todas las actividades de tratamiento (Artículo 2, apartado 20, de la DGA).

En caso de reutilización no autorizada de datos no personales, la DGA atribuye al usuario de los datos en cuestión la responsabilidad de informar a las personas jurídicas cuyos derechos o intereses puedan verse perjudicados (Artículo 5, apartado 5, de la DGA). Por el contrario, la reutilización no autorizada de datos personales se rige por el RGPD. El organismo del sector público seguirá siendo, por lo general, el responsable del tratamiento en virtud del RGPD, ya que determina las condiciones del tratamiento de datos dentro del SPE. Sin embargo, la evaluación de la responsabilidad del tratamiento en virtud del RGPD es siempre funcional y depende del contexto. En consecuencia, si un incidente de seguridad en un SPE da lugar a una violación de datos que afecte tanto a datos personales como a datos no personales, tanto el usuario de datos como el organismo del sector público pueden tener responsabilidades frente a las personas jurídicas y físicas afectadas, así como obligaciones de notificación a las autoridades nacionales competentes.

Para reducir las ambigüedades, los acuerdos de tratamiento de datos entre los organismos del sector público y los usuarios de datos deberían definir explícitamente el alcance de las responsabilidades de cada parte y establecer mecanismos para la atribución de responsabilidades, así como para la resolución de litigios, especialmente en lo que se refiere a las reclamaciones de indemnización. Dichos acuerdos son esenciales para evitar la duplicación de obligaciones de información y reducir la complejidad operativa y jurídica.

Además, el hecho de basarse en la variabilidad contractual y jurisdiccional entre los Estados miembros. Por ejemplo, si un usuario de datos de un Estado miembro A comete una infracción grave al acceder a datos sensibles dentro de una SPE alojada por un organismo del sector público en un Estado miembro B, el usuario debería, en principio, aceptar la jurisdicción del Estado miembro B para la resolución de litigios (Considerando 20 de la DGA). Sin embargo, el alcance y el efecto de las sanciones no pecuniarias, como la exclusión temporal del acceso a determinados datos o SPE, se limitan a la jurisdicción de la autoridad que las impone y no se aplican automáticamente en todos los Estados miembros. A falta de mecanismos de reconocimiento mutuo o de normas de interoperabilidad jurídica, dicha fragmentación corre el riesgo de socavar la confianza y la seguridad jurídica en el intercambio transfronterizo de datos. En última instancia, esto debilita el objetivo de crear un marco europeo coherente de gobernanza de datos.

4 CONCLUSIONES

Los marcos horizontales actuales que regulan la ciberseguridad y la protección de datos no logran establecer un régimen de responsabilidad armonizado y adaptado a los entornos de intercambio de datos federados y transfronterizos. Estos marcos se basan en gran medida en acuerdos contractuales, que deben adaptarse a la estructura organizativa específica, el perfil de riesgo, la sensibilidad de los datos y las obligaciones de cumplimiento de cada sector. Este análisis pone de relieve varias complejidades y lagunas que dificultan la creación de marcos de responsabilidad coherentes para los espacios de datos y la aplicación efectiva de las obligaciones de la UE en materia de ciberseguridad.

La NIS2 establece un marco básico de responsabilidad para la gobernanza de la ciberseguridad; sin embargo, no delimita la responsabilidad en situaciones en las que las vulnerabilidades se propagan a través de infraestructuras interconectadas de intercambio de datos. Del mismo modo, el enfoque funcional del RGPD para la asignación de funciones (por ejemplo, responsables del tratamiento, responsables conjuntos y encargados del tratamiento) no se ajusta perfectamente a los modelos de gobernanza previstos en los espacios de datos o en la DGA. Estas cuestiones son especialmente notorias en infraestructuras complejas de intercambio de datos, donde la identificación y el cumplimiento de funciones y responsabilidades requieren mecanismos de gobernanza sólidos.

Las iniciativas transfronterizas se enfrentan a una complejidad aún mayor debido a las interpretaciones nacionales divergentes de las distintas legislaciones, en particular la NIS2. Los retos operativos, como la aplicación de sanciones no pecuniarias limitada a una jurisdicción concreta, así como los alcances variables y los requisitos de notificación fragmentados, suponen una carga para las iniciativas que buscan establecer procesos eficaces de respuesta a incidentes. Las entidades dentro y fuera del ámbito de aplicación de estas normativas pueden verse en la necesidad de colaborar durante los incidentes de seguridad, lo que subraya la necesidad de un marco de gobernanza mínimo viable que armonice las obligaciones básicas. Si bien la mayoría de los espacios de datos europeos hacen hincapié en el cumplimiento del RGPD y las garantías de privacidad, la preparación para los incidentes de ciberseguridad y el cumplimiento de las obligaciones de la NIS2 siguen estando poco desarrollados.

Por último, la atribución de la responsabilidad jurídica en los espacios de datos dependerá de su forma organizativa, de los acuerdos contractuales y del contexto jurisdiccional. A falta de orientaciones armonizadas a nivel de la UE, estas incertidumbres pueden socavar la confianza y desalentar la participación en los ecosistemas de intercambio transfronterizo de datos. El establecimiento de un marco de gobernanza coherente que defina los principios básicos para la preparación en materia de ciberseguridad, la coordinación de incidentes y la atribución de responsabilidad, junto con códigos de conducta específicos para cada sector y modelos contractuales normalizados, contribuiría a abordar estos retos y a reforzar la seguridad jurídica.

Estas medidas son esenciales no solo para salvaguardar la integridad y la resiliencia de las infraestructuras de intercambio de datos, sino también para mitigar e, idealmente, prevenir los posibles daños y responsabilidades derivados de una filtración de datos cada vez más inevitable.