INTERNATIONAL JOURNAL OF DIGITAL LAW – IJDL
v. 7 · e706 · 2026 – DOI: 10.47975/ijdl.v7.1348

IJDL

International Journal of DIGITAL LAW

NUPED
Núcleo de Pesquisas em Políticas Públicas e Desenvolvimento Humano da PUCPR

FORUM

International Journal of Digital Law – IJDL
DOI: 10.47975/ijdl.v7.1348

La protección de datos mediante la seudonimización fuerte

Data protection using strong pseudonymization

Antoni Roig Batalla*
Universidad Autónoma de Barcelona (Cerdanyola del Vallès, España)
antoni.roig@uab.cat
https://orcid.org/0000-0002-4760-9361

Recebido/Received: 16.04.2026 / April 16th 2026
Aprovado/Approved: 27.06.2026 / June 27th 2026

Resumen: La seudonimización es una garantía frente a los riesgos de violación de la seguridad de los datos personales (Data Breach) y permite demostrar un nivel adecuado de protección de los datos personales. Si nos centramos en sus funciones, la seudonimización facilita el cumplimiento de los principios de protección de datos por el diseño y por defecto (artículo 25 RGPD) y de seguridad (artículo 32 RGPD). En cambio, hasta ahora, se daba menos relevancia a su tercera función de garantía del cumplimiento de los principios de protección de datos (artículo 5 RGPD), quizá con la salvedad de los principios de minimización de los datos y de conservación limitada de la información. Nuestra hipótesis es que los seudónimos van a ser cada vez más usados, apoyados en la base legal del interés legítimo (artículo 6.1 f) RGPD). También va a contribuir a este renacer la propuesta del propio CEPD de interacción entre el derecho a la protección de datos y el derecho a la competencia. Como veremos, la inteligencia artificial podría reducir o incluso eliminar la capacidad de protección de los seudónimos en un momento en el cual renace la apuesta jurídica por la seudonimización.

Palabras clave: Protección de datos. Seudonimización. Inteligencia artificial. Anonimización. Privacidad por el diseño.

Abstract: Pseudonymization avoids data breaches and is an adequate safeguard for data protection. Among its goals, pseudonymization assures due compliance of privacy by design and by default principles (articles 25 GDPR) and security (article 32 GDPR). So far, less attention has been paid to its safeguard of data protection principles (article 5 GDPR), except for data minimization and limited retention of information. We expect pseudonyms to be increasingly used, with the legal justification of legitimate interest (article 6.1 f) GDPR). The European Committee of Data Protection's (ECDP)

Como citar este artigo/*How to cite this article*: ROIG BATALLA, Antonio. La protección de datos mediante la seudonimización fuerte. *International Journal of Digital Law*, Belo Horizonte, v. 7, e706, 2026. DOI: 10.47975/ijdl.v7.1348.

* Profesor Titular de Derecho Constitucional de la Universidad Autónoma de Barcelona (Cerdanyola del Vallès, España). Doctor en Derecho por la Universidad Autónoma de Barcelona. Investigador del Instituto de Derecho y Tecnología (IDT-UAB). E-mail: Antoni.roig@uab.cat.

proposal of interaction between data protection and consumer protection should also increase the use of pseudonyms. However, as we will explain, IA might reduce or even erase pseudonyms' safeguards just when the lawmaker opts for them.

Keywords: Data protection. Pseudonymization. Artificial intelligence. Anonymization. Privacy by design.

1 Introducción: una seudonimización fuerte requiere contexto, es decir un espacio de seudonimización

Siguiendo la definición del Reglamento General de Protección de Datos (RGPD), en su artículo 4.5, la seudonimización es una técnica equilibrada que aúna la reducción de riesgos de identificación con la eficacia del tratamiento de los datos.[1] Las Recomendaciones 1/2025, de 16 de enero, del Comité Europeo de Protección de Datos (en adelante, CEPD) desarrollaron su función de garantía de la protección de datos.[2] También va a contribuir a este renacer la propuesta del propio CEPD de interacción entre el derecho a la protección de datos y el derecho a la competencia.[3] A diferencia de la anonimización, un pseudónimo es un dato personal y sólo cumple como garantía de los principios del RGPD en su versión fuerte, que queremos contribuir a esbozar en este trabajo.[4] Si no se consigue reforzar el uso efectivo

1 Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos, en adelante, RGPD). Puede verse la voz de Luca Tosoni. TOSONI, Luca. Article 4(5): Pseudonymisation. In: KUNER, Christopher; BYGRAVE, Lee A.; DOCKSEY, Christopher (eds.) *The European Union General Data Protection Regulation (GDPR):* a *commentary.* Oxford: Oxford University Press, 2020. DOI: https://doi.org/10.1093/oso/9780198826491.001.0001.

2 CEPD. *Guidelines 01/2025 on Pseudonymisation.* Bruxelas: European Data Protection Board, 2025. Adoptado el 16 ene. 2025. La Agencia de la Unión Europea para la ciberseguridad (ENISA), pese a disponer de varios estudios sobre las técnicas habituales y avanzadas de seudonimización, venía reclamando prestar más atención a su relación con el art. 25 RGPD. Así, puede verse, por ejemplo, AGENCIA DE LA UNIÓN EUROPEA PARA LA CIBERSEGURIDAD (ENISA). *Pseudonymisation techniques and best practices: recommendations on shaping technology according to data protection and privacy provisions.* [S.l.]: ENISA, 2019. p. 7.

3 CEPD, *Position paper on Interplay between data protection and competition law*, adoptado el mismo 16 de enero de 2025 que las Recomendaciones 1/2025. Puede verse un ejemplo en la STJUE (Gran Sala) de 4 de julio de 2023, Caso Meta Platforms y Bundeskartellamt (C-252/21). La conectividad del IoT (Internet de las Cosas) también requiere aproximar la protección de datos y la protección del consumidor: puede verse, por ejemplo, DONADIEU, Gwenaëlle. Le RGPD et la protection de la vie privée face à l'essor des objets connectés. Tic & société, v. 15, n. 2-3, p. 217-239, 2022. DOI: https://doi.org/10.4000/ticetsociete.6720.

4 El caso Thin resuelto por la autoridad italiana de protección de datos puede ilustrar sobre un uso, sin base legal en el RGPD, de datos seudonimizados, es decir no anonimizados (Garante per la protezione dei dati

del seudónimo, se estará dando una falsa sensación de seguridad y se podrían incrementar significativamente los riesgos para los derechos de los interesados.[5]

Como es sabido, la seudonimización reduce los riesgos para la persona interesada al no atribuir un dato a un individuo, sin por ello perder la capacidad para el análisis y el tratamiento de la información.[6] Es precisamente esta capacidad para el uso abierto o la reutilización la que potencia su renacer. Por otro lado, los datos seudonimizados son los de una persona natural identificable, y por ello son datos personales.[7] La seudonimización fuerte requiere contexto. En primer lugar, no sólo se protege la identidad en el mundo real del sujeto titular de los datos, sino también los identificadores indirectos o únicos que podrían llevar a identificar al interesado.[8] La perspectiva tradicional de la seudonimización —débil— considera crucial la protección de la información adicional. Así, se sostiene la necesidad de adoptar medidas de seguridad adecuadas y de separar la información adicional de los datos seudonimizados. Esta aproximación es limitada e incluso puede relajar las obligaciones del responsable o encargado de los datos. Veamos primero los límites de esta postura para después mencionar la relajación en las obligaciones del responsable.

La seudonimización débil no cumple las funciones que le reserva la regulación de la economía de datos. En primer lugar, la definición del contexto debe insertarse en el ámbito general de las medidas de seguridad y del deber de responsabilidad proactiva.[9] En segundo lugar, hay que cambiar la perspectiva: no se trata de la robustez o de la fragilidad de los seudónimos como tales; la seudonimización, por sí sola, no es suficiente garantía del principio de protección de datos por el

personali, Procedimiento de 1 de junio de 2023, proyecto Thin). Con todo, aunque la seudonimización suele diferenciarse de la anonimización en muchos ordenamientos, la existencia de un tercer concepto, la desidentificación, requerirá una armonización internacional (véase la mesa redonda del G7 al respecto, G7 Italia 2024, *Roundtable of G7 Data Protection and Privacy Authorities*. Reducing identifiability in cross-national perspective: Statutory and policy definitions for anonymization, pseudonymization, and deidentification in G7 jurisdictions, 11 de octubre de 2024).

5 AGENCIA DE LA UNIÓN EUROPEA PARA LA CIBERSEGURIDAD (ENISA). *Recommendations on shaping technology according to GDPR provisions: an overview on data pseudonymisation.* [S.l.]: ENISA, 2018. p. 6.

6 "La seudonimización es una de las distintas técnicas de <<desidentificación>> (como la agregación, la ofuscación y el enmascaramiento, etc.) destinadas a eliminar la asociación entre el conjunto de datos de identificación y el sujeto de los datos" AGENCIA DE LA UNIÓN EUROPEA PARA LA CIBERSEGURIDAD (ENISA). *La adopción de técnicas de seudonimización: el caso del sector sanitario.* [S.l.]: ENISA, 2022. p. 8). Esta definición coincide con el artículo 4, apartado 5 del RGPD.

7 Considerando 26 del RGPD. Grupo de trabajo del artículo 29, *Dictamen 4/2007*, sobre el concepto de datos personales (WP 136,) adoptado el 20 de junio de 2007, 18; también, AEPD/EDPS, 10 malentendidos relacionados con la anonimización, disponible en https://www.aepd.es/guias/10-malentendidos-anonimizacion.pdf.

8 Un identificador directo sería, por ejemplo, el nombre o una imagen del interesado; cuando hablamos de un identificador indirecto nos referimos, en cambio, a un número de teléfono, un correo electrónico o un identificador único asignado por un responsable (Data Protection Commission (Irlanda), *Guidance on Anonymisation and Pseudonymisation*, 2019, p. 4-5).

9 Considerando 28 del RGPD.

diseño o por defecto, de la seguridad del tratamiento.[10] Ni siquiera el cifrado puede considerarse una técnica equivalente a una anonimización.[11] Hay que aceptar la realidad de que un tercero, que no sea el responsable ni el encargado de los datos, pueda re-identificar a una persona a partir del seudónimo, y ello sin disponer de la información adicional.[12] En efecto, los identificadores personales, como el nombre, la dirección de correo electrónico o el número de la seguridad social, entre otros, aislados o combinados entre ellos, pueden ayudar a re-identificar a una persona sin necesidad de disponer de la información adicional (claves o desencriptación). En último término dependerá del contexto: la presencia de identificadores no siempre supondrá que el interesado es identificado o identificable; pero tampoco la ausencia de identificadores garantiza, sin más, que la información no pueda servir para vincularla finalmente con una persona. En definitiva, la protección deberá tener en cuenta esta posibilidad: según el contexto, el nivel de seudonimización deberá ser fuerte. La seudonimización no cumple con los principios del art. 5 RGPD cuando su nivel de protección es inadecuado, a pesar de ser una medida expresamente mencionada en el art. 25 RGPD.[13] Urge pues reforzar los seudónimos más allá de la protección de la información adicional.

Por otro lado, los seudónimos débiles pueden relajar las obligaciones de los responsables o encargados de los datos. Así cuando hay que valorar si el nuevo uso de los datos es compatible con la finalidad inicialmente consentida, el hecho de ser un seudónimo puede erróneamente llevar a concluir que se han adoptado las medidas adecuadas. También, en caso de violación de la seguridad de los

---

10 Las técnicas básicas de seudonimización son un contador, un número aleatorio, una función resumen (hash) un código de autenticación de mensaje resumido (HMAC) y el cifrado (AGENCIA DE LA UNIÓN EUROPEA PARA LA CIBERSEGURIDAD (ENISA). *Recommendations on shaping technology according to GDPR provisions: an overview on data pseudonymisation.* [S.l.]: ENISA, 2018. p. 9-10). Puede verse una descripción sencilla en AGENCIA DE LA UNIÓN EUROPEA PARA LA CIBERSEGURIDAD (ENISA). Data Pseudonymisation: Advanced Techniques & Use Cases: technical analysis of cybersecurity measures in data protection and privacy. [S.l.]: ENISA, 2021, apartado 2.2. Sobre el hash como técnica de seudonimización, AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS; SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS (AEPD/EDPS). Introducción al hash como técnica de seudonimización de datos personales. [S.l.]: AEPD/EDPS, 2019. Para que el hash cumpla una función de anonimización, el análisis de riesgos debe incluir las medidas organizativas que garantizan la eliminación de la información que permita la re-identificación y una garantía de robustez más allá de la vida esperada de los datos de carácter personal (AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS; SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS (AEPD/EDPS). Introducción al hash como técnica de seudonimización de datos personales. [S.l.]: AEPD/EDPS, 2019. p. 22-23).

11 AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD). *Orientaciones para la validación de sistemas criptográficos en la protección de datos.* [S.l.]: AEPD, 2023. p.2. En cambio, el cifrado es adecuado para la seudonimización (p.12).

12 La seudonimización no es una técnica de anonimización, sino una técnica de seguridad que debe ir acompañada de medidas adicionales para anonimizar, como la generalización o la eliminación de los datos originales (por ejemplo, en European Medicines Agency, *External guidance on the implementation of the European Medicines Agency policy on the publication of clinical data for medicinal products for human use*, de 15 de octubre de 2018, EMA/90915/2016, versión 1.4, p.41.

13 AGENCIA DE LA UNIÓN EUROPEA PARA LA CIBERSEGURIDAD (ENISA). *Recommendations on shaping technology according to GDPR provisions: an overview on data pseudonymisation.* [S.l.]: ENISA, 2018. p. 11.

datos personales, puede creerse que la seudonimización débil reduce el riesgo de re-identificación. Más aún, los derechos de acceso, rectificación y supresión de datos (arts. 15-20 RGPD) no serían aplicables si el encargado no puede identificar a los usuarios.[14]

Las Recomendaciones 1/2025 del CEPD concretan algunos conceptos relevantes para la seudonimización fuerte.[15] Se incluye en las mismas un glosario que concreta la definición del art. 4.5 RGPD: la atribución de datos seudonimizados a la persona interesada se describe como el proceso que los vincula a una persona ya identificada; a su vez, la transformación por seudonimización consiste en el procedimiento mediante el cual se modifican los datos originarios de manera que el resultado no pueda ser atribuible a ninguna persona sin mediar información adicional; finalmente, esta última es la que permite la atribución de datos seudonimizados a una persona identificada o identificable. La información adicional incluye las claves de seudonimización —algoritmos de encriptación o tablas— (*pseudonymisation secrets*) y los datos originarios, y debe guardarse por separado, asegurando la confidencialidad y evitando usos no autorizados. Hay que evitar, así, que la información adicional entre en el dominio de la seudonimización. Además, la modificación de los datos originarios dependerá del ámbito de seudonimización: cuanto menor sea este último, menos deberán modificarse los datos originarios. También es interesante la referencia a casi-indicadores, es decir datos que permiten atribuir la información a una persona sin necesidad de revertir la transformación seudonimizadora. En ese caso, lo mejor es suprimir ese dato o modificarlo por generalización o aleatoriedad.

Otra contribución interesante es la clasificación de los seudónimos por categorías: los seudónimos de personas son los más vulnerables y obligan a medidas de protección a largo plazo de las claves; en cambio, los seudónimos de relación —cliente, empleado— deben conservarse únicamente mientras dure la relación comercial o contractual; finalmente, los seudónimos creados para cada transacción reducen mejor los riesgos y contribuyen mejor a los principios de protección de datos. En resumen, debe preferirse la seudonimización aleatoria antes que la determinista: la primera utiliza un seudónimo diferente para los mismos datos, mientras que la segunda usa siempre el mismo seudónimo para los mismos datos.[16] En cuanto a los

[14] AGENCIA DE LA UNIÓN EUROPEA PARA LA CIBERSEGURIDAD (ENISA). *Recommendations on shaping technology according to GDPR provisions: an overview on data pseudonymisation.* [S.l.]: ENISA, 2018. p. 16-17.

[15] Así, María Arias Pou incluye a la seudonimización entre las definiciones nuevas del RGPD en su capítulo de libro III. Definiciones a efectos del Reglamento General de Protección de Datos. In.: PIÑAR MAÑAS, José Luis(dir.); ÁLVAREZ CARO, María; RECIO GAYO, Miguel (coords.) *Reglamento General de Protección de Datos: hacia un nuevo modelo europeo de privacidad.* Madrid: Editorial Reus, 2020. p.115-133, esp. 127-129.

[16] AGENCIA DE LA UNIÓN EUROPEA PARA LA CIBERSEGURIDAD (ENISA). *La adopción de técnicas de seudonimización: el caso del sector sanitario.* [S.l.]: ENISA, 2022, p.10.

derechos de los interesados, se sostiene que toda reversión de la seudonimización no autorizada es una violación de la seguridad de los datos personales (*data protection breach*).

Ello no es suficiente para obtener una seudonimización fuerte. La principal contribución de las Recomendaciones de 2025 es el llamado ámbito o dominio de la seudonimización (*pseudonymisation domain*): se trata del espacio en el cual el responsable o encargado relaciona el dato seudonimizado con el de una persona específica. El cambio es notable, por ejemplo, en relación con el estudio de ENISA de 2022 sobre la seudonimización, cuyos casos de uso no profundizan en el contexto, ni en los encargados, ni en el tratamiento. De hecho, curiosamente, ENISA ya advertía en un estudio previo de 2019 sobre la seudonimización que, para entender la incidencia de la seudonimización sobre el proceso de datos, debía realizarse un análisis legal completo de la situación del caso concreto.[17] ENISA no abordó tampoco esta tarea en su siguiente estudio sobre seudonimización, de 2022, cosa que no debería extrañar dado el carácter eminente técnico de esta institución. El ámbito de la seudonimización incluye, esta vez sí, a las personas que actúan bajo la autoridad del responsable o del encargado del tratamiento, otras personas físicas o jurídicas, autoridades y agencias, así como los recursos tecnológicos e informativos de éstos. La hipótesis de la cual parte el CEPD es que la adecuada gestión del contexto de la seudonimización permitirá reducir los riesgos y garantizar el cumplimiento de los requisitos de la protección de datos y los principios de protección por el diseño y por defecto. Por consiguiente, la seudonimización fuerte seguiría siendo una garantía válida que, además, podría servir como medida suplementaria para las transferencias a países terceros.

2 La protección mediante seudónimos de la confidencialidad, del principio de minimización de datos y de la limitación de finalidad

2.1 La protección de la confidencialidad

Empezaremos a estudiar la protección mediante seudónimos de los principios de protección de datos con uno de los pocos supuestos que ha merecido la atención hasta el momento: la confidencialidad.[18] Imaginemos que un hospital se

[17] AGENCIA DE LA UNIÓN EUROPEA PARA LA CIBERSEGURIDAD (ENISA). *Data Pseudonymisation*: Advanced Techniques & Use Cases. Technical analysis of cybersecurity measures in data protection and privacy. [S.l.]: ENISA, 2021, p. 7, nota 3, y p.10. Así, se sostiene la necesidad de concretar quién es la "entidad seudonimizadora", sea ésta un controlador, un encargado, un tercero o el interesado.

[18] PUYOL MONTERO, Javier. Los principios del derecho a la protección de datos. In: PIÑAR MAÑAS, José Luis (dir.); ÁLVAREZ CARO, María; RECIO GAYO, Miguel (coords.). *Reglamento General de Protección de Datos*: hacia un nuevo modelo europeo de privacidad. Madrid: Editorial Reus, 2016. p. 135-150.

dirige a otro centro para que le confirme si dispone efectivamente de la versión más actualizada del expediente médico de un paciente. Para evitar que los datos personales generales y médicos del cliente se vean comprometidos, se utiliza un seudónimo. Sin embargo, no todos los seudónimos ofrecen la misma protección: la simple sustitución del contenido por un seudónimo único —determinista— no es una solución satisfactoria, pues sería fácil volver a identificar al interesado.[19] Por ello, creemos acertada la opción de ENISA por un árbol o una cadena de seudónimos. La primera conclusión que deberíamos extraer es que un seudónimo único vinculado a una persona es el más vulnerable y raramente cumplirá con la exigencia de robustez requerida. Por mucho que el artículo 25 RGPD mencione la seudonimización, debemos interpretar que únicamente el seudónimo fuerte cumple como garantía adecuada de los principios de la protección de datos. Y un seudónimo único o determinista no es fuerte.

2.2 La protección del principio de minimización

Imaginemos ahora que una empresa quisiera gestionar un proceso de selección de proveedores o de personal mediante seudónimos, para garantizar el cumplimiento del principio de minimización de datos. Para ello, podría crear un centro de verificación encargado de la gestión de los seudónimos. Esta solución no es satisfactoria y deberá preferirse un modelo descentralizado de seudonimización: la agencia podría entregar a los candidatos o proveedores una aplicación que les permitiera realizar ellos mismos la seudonimización, y que garantizase que los documentos adicionales requeridos se correspondiesen luego con los inicialmente indicados. De esta manera incorporamos un segundo criterio para la seudonimización fuerte: no sólo hay que evitar el seudónimo único, también el centro único de verificación. Recuérdese, finalmente, la sugerencia del Considerando 8 del RGPD, según el cual deberán usarse los algoritmos, cuando ello sea posible técnicamente, "(...) sin que sea necesaria la transmisión entre las partes ni la copia superflua de los datos brutos o estructurados". Sin transmisión de los datos, no es necesario usar ningún seudónimo; y el seudónimo más seguro siempre es el que no se usa. Por consiguiente, antes de incorporar una seudonimización, hay que valorar la posibilidad de simplemente evitar la transmisión de los datos.

[19] PARK, Hyun A. The DtMin Protocol: Implementing Data Minimization Principles in Medical Information Sharing. *Electronics*, Basel, v. 14, n. 8, 1501, 30 páginas, 2025. DOI: https://doi.org/10.3390/electronics14081501. De hecho, las soluciones técnicas para garantizar el principio legal de minimización de los datos suelen ser bastante complejas. Véase, por ejemplo, CONTE, Raffaele et al. Privacy-by-design and minimization within a small electronic health record. The Health360 case study. *Applied Sciences*, v. 12, n.17, 8441, 13 páginas, 2022. DOI: https://doi.org/10.3390/app12178441.

2.3 La protección de la limitación de finalidad

La protección de la limitación de finalidad también puede lograrse mediante una seudonimización fuerte.[20] Los seudónimos pueden ayudar a la compatibilidad de finalidades (art. 6.4 RGPD) cuando existe interés legítimo. Imaginemos, así, que un equipo técnico de seguridad tiene acceso a un repositorio central de datos de comunicaciones seudonimizadas. Los técnicos únicamente pueden buscar por fechas, origen o destinatarios. Si se obtienen indicios suficientes, entonces el equipo técnico podrá requerir la IP del personal identificado como razonablemente sospechoso. Ello permite realizar un control más exhaustivo, pero únicamente cuando haya indicios razonables para ello; no de entrada. En definitiva, para considerar la nueva finalidad compatible con el originario, sin que se esté realizando un perfil de los clientes (art. 4, apartado 4 del RGPD), los datos deben procesarse de manera que los analistas no puedan individualizar los atributos de los interesados concretos. Reservar el control más intenso cuando existan indicios razonables es una buena práctica; sin embargo, es una excepción. La regla general para proteger la limitación de propósito debería ser el uso de seudónimos – fuertes – de transacción.

La limitación de la finalidad exige dar un paso más en la robustez de la seudonimización. En este sentido, los estudios de ENISA y las Recomendaciones 1/2025 del CEPD aconsejan el uso de los seudónimos de transacción.[21] En efecto, en la llamada codificación polimorfa y seudonimización (PEP, por sus siglas en inglés), los datos personales se cifran de manera que no hay que prefigurar quién puede descifrarlos. El texto puede entonces transformarse posteriormente en otra versión de cifrado que únicamente pueda descifrar el destinatario. Además, a una misma persona se le asignan seudónimos diferentes para cada tercero que solicite acceso a los datos, lo cual preserva la identidad del interesado y evita que se vinculen los datos parciales obtenidos a una concreta persona. Así pues, además de evitar los seudónimos únicos y los certificadores centralizados, los seudónimos de transacción serían un requisito para la seudonimización fuerte.

La certificación por tercero podría ser una solución alternativa al seudónimo de transacción. En efecto, las credenciales basadas en atributos (ABC, por sus siglas en inglés) son útiles para preservar la identidad del interesado a pesar de permitir

[20] Sobre el principio de limitación de finalidad, puede verse la Tesis de Maximilian von Grafestein. The Principle of Purpose Limitation in Data Protection Laws. The Risk-based Approach, Principles, and Private Standards as Elements for Regulating Innovation, Nomos, Baden, 676 páginas, 2018. Más recientemente, un intento de salvar la eficacia técnica del principio jurídico en FINCK, Michèle; BIEGA, Asia J. Reviving Purpose Limitation and Data Minimisation in Data-Driven Systems, *Technology and Regulation*, p. 44-61, 2021. DOI: https://doi.org/10.71265/z7r0t122.

[21] AGENCIA DE LA UNIÓN EUROPEA PARA LA CIBERSEGURIDAD (ENISA). *Ingeniería de compartición de datos personales: casos de uso y tecnologías emergentes.* Versión 1. [S.l.]: ENISA, 2023, esp. p. 14-15 y p. 21-22.

el acceso a ciertos atributos.[22] Así, un usuario envía ciertos atributos como, por ejemplo, la residencia, el permiso de conducir y la mayoría de edad a una entidad de confianza, que los valida y firma digitalmente. Los certificados podrán entonces enviarse a terceros. En este sentido, la CNIL francesa recomienda la autenticación basada en atributos, con un tercero de confianza, para cumplir con la obligación de verificación de edad sin exponer por ello la identidad del interesado. Esta es también la solución de la cartera digital europea.

La legislación europea de uso secundario de los datos de salud electrónicos para fines distintos de la prestación de asistencia sanitaria (recetas, dispensación de medicamentos, servicios sociales y administrativos) puede acelerar la implantación de seudónimos.[23] Siempre que se respeten los fines para los que se pueden tratar datos de salud electrónicos para uso secundario (art. 53 EEDS), las solicitudes de acceso deberán incluir "una descripción explicativa de si los datos de salud electrónicos deben ponerse a disposición en un formato seudonimizado o anonimizado (...)" (art. 67.2, letra e) EEDS). Pero lo más significativo es que, en el mismo precepto puede leerse a continuación: "en caso de un formato seudonimizado, [deberá incluirse] una justificación de la razón por la que el tratamiento no puede realizarse mediante datos anonimizados". Es decir, por defecto, la garantía deberá ser la anonimización, mientras que la seudonimización requerirá justificar la imposibilidad de anonimizar. Así, deberá existir "una justificación suficiente de que el fin no puede alcanzarse con datos anonimizados" (art. 68.1, letra c) EEDS). Por ello, los datos de salud electrónicos para uso secundario se proporcionarán en formato anonimizado, cuando los fines del tratamiento lo permitan (art. 66.2 EEDS) y si se demuestra suficientemente que dichos fines no pueden alcanzarse, entonces se proporcionará el acceso a dichos datos en formato seudonimizado, sin incluir la información adicional necesaria para revertir la seudonimización (art. 66.3 EEDS). Con el tiempo podrá verse si la anonimización es finalmente la regla general, como pretende el legislador o bien la seudonimización adquiere relevancia en el uso secundario de los datos de salud. En cualquier caso, el principio de limitación de finalidad ya requiere ineludiblemente una seudonimización más fuerte —si cabe— que la minimización de los datos y la confidencialidad, con la incorporación del tercer requisito: el seudónimo de transacción.

---

22 Sobre las credenciales basadas en atributos, puede verse el apartado 5.3.1. del estudio de ENISA, *Ingeniería de la protección de datos*. De la teoría a la práctica, enero 2022.

23 Sobre el uso primario y secundario de los datos de salud electrónicos, véase el art. 2.2 letra d) y e) del Reglamento (UE) 2025/327 del Parlamento Europeo y del Consejo de 11 de febrero, 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). Puede verse, al respecto, 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*, v. 2, p.525-551, 2024.

3 La protección de la calidad de los datos y la protección suplementaria en las transacciones internacionales

Una vez estudiada la garantía mediante seudónimo de los principios de protección de datos más habituales —minimización de datos y limitación de finalidad— conviene ahora ampliar el ámbito de la protección a los demás principios. Empezaremos por el principio de calidad de los datos.[24] Imaginemos que un laboratorio médico envía un mensaje con los resultados de unas análisis al teléfono móvil de un cliente. Para evitar los errores debidos a nombres homónimos o a direcciones similares, cada muestra es etiquetada con un seudónimo que puede tener muchos atributos del interesado. Además de garantizar el anonimato de las muestras cuando se realizan las pruebas, la precisión resultante es mayor y se evitan envíos a personas equivocadas. No añadimos, con todo, ningún requisito nuevo a la seudonimización fuerte.

Más relevante se nos antoja la contribución de la seudonimización como garantía suplementaria de los principios y requisitos de la protección de datos en las transferencias internacionales.[25] Concretamente, la ventaja ofrecida por la seudonimización fuerte consiste en contribuir a preservar las garantías adecuadas que requiere el artículo 46 RGPD para las transferencias internacionales de datos personales. Este es un supuesto interesante, pues muestra el cambio notable del seudónimo, anteriormente limitado a su función de seguridad, y ahora dotado de una nueva versatilidad que le permite apuntalar principios y requisitos insospechados. Por ejemplo, un uso instrumental de la seudonimización, en relación con la evaluación de impacto, sería el siguiente: una empresa utiliza los servicios de un proveedor de servicios de un país tercero, fuera del ámbito de la Unión Europea y del EEA. Aunque existe un contrato entre la empresa y el proveedor de servicios que contiene cláusulas tipo de protección de datos de acuerdo con el artículo 46, apartado 2, letra c) del RGPD, la evaluación de impacto realizada determina que el proveedor de servicios no cumplirá con todos los requisitos debido a una regulación nacional menos garantista.[26] Se requiere para ello un análisis legal y factual para concretar potenciales atacantes relevantes, que no se reduce a individuos y empresas, sino que puede incluir administraciones públicas.[27] Pues bien, para evitar esto,

[24] TERWANGNE, Cécile de; BYGRAVE, Lee A. Article 5: Principles relating to processing personal data. In: KUNER, Christopher; BYGRAVE, Lee A.; DOCKSEY, Christopher (dirs.) *The European Union General Data Protection Regulation: a commentary*. Oxford: Oxford University Press, 2020. p.309-320. DOI: https://doi.org/10.1093/oso/9780198826491.003.0034.

[25] NAEF, Tobias. *Data Protection without Data Protectionism*. The Right to Protection of Personal Data and Data Transfers in EU Law and International Trade Law. Zurich: Springer, 2023.

[26] Ejemplo 9 del Anexo de la Recomendación 1/2025 del CEPD.

[27] Puede ponerse esto en relación con el Caso Schrems II, del TJUE, Caso C-311/18 Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems, de 16 de julio de 2020. El TJUE postuló

los cuestionarios de los empleados que deben enviarse al proveedor de servicios son encriptados de manera que, si las autoridades del país tercero obtienen los datos transferidos del proveedor nacional, no podrán atribuirlos a una persona concreta. La encriptación es una técnica de seudonimización. Por consiguiente, la seudonimización añade una protección suplementaria que permite concluir que se cumplen finalmente las garantías adecuadas exigidas en el artículo 46 RGPD para las transferencias.

Este uso instrumental de la seudonimización para garantizar la adecuación en las transferencias internacionales de datos no es nuevo. Así, en las Recomendaciones del CEPD 01/2020, sobre medidas suplementarias de las herramientas de transferencia para asegurar el cumplimiento del nivel adecuado de la Unión Europea de protección de los datos, se incluye un caso de uso 2 sobre transferencia de datos seudonimizados.[28] Los datos son enviados seudonimizados de manera que los datos personales no pueden ser individualizados sin la información adicional. Ésta se encuentra en posesión del exportador, en un espacio separado y protegido por medidas técnicas y organizativas. Esto debería haber sido suficiente para confirmar que se trata de una seudonimización fuerte. Sin embargo, se advierte que lo relevante es que el encargado llegue a la conclusión, en su análisis, que los datos seudonimizados no pueden vincularse a los interesados, teniendo en cuento los datos que se encuentran a disposición o que puede usar el receptor, en este caso un instituto de investigación. Se afirma además la necesidad de tener en cuenta que ciertas instituciones públicas pueden tener recursos técnicos y financieros muy importantes que pueden usar para re-identificar sin necesidad de disponer de la información adicional.[29] El cambio de perspectiva es notable: la protección y aislamiento de la información adicional no es suficiente; hay que asegurarse también que no se puede reidentificar a los interesados sin necesidad de la información adicional, teniendo en cuenta las capacidades no sólo de actores económicos con muchos recursos, sino también de actores públicos. Este nuevo requisito para la seudonimización fuerte es quizá el más importante: hay que tener en cuenta las capacidades de re-identificación de los actores económicos con

además la responsabilidad no sólo del encargado, sino también de las autoridades nacionales e incluso del CEPD. Con ello, se quería fomentar una actitud más proactiva que culminó con unas recomendaciones sobre la metodología a emplear en tales casos (EDPB, *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data*, versión 2.0, de 18 de junio de 2021). Sin embargo, sigue faltando una metodología de evaluación basada en el riesgo. Lo más parecido, hasta el momento, es la herramienta del ICO británico que clasifica los datos personales transferibles en función del nivel de riesgo (ICO, Transfer Risk Assessment Tool).

[28] CEPD. *Recomendaciones 01/2020, on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data*, versión 2.0, adoptado el 18 de junio de 2021.

[29] CEPD. *Recomendaciones 01/2020, on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data,* versión 2.0, adoptado el 18 de junio de 2021. pár. 88.

muchos recursos y también de las instituciones públicas para asegurarse que se dispone de un seudónimo fuerte.

4 La protección del derecho de acceso y del derecho a la portabilidad de los datos

La protección del derecho al acceso y del derecho a la portabilidad de los datos no requiere de seudónimos fuertes. El Reglamento de Datos (en adelante R.D.) muestra además una clara preferencia por la anonimización. El supuesto más recomendable de seudónimo garante de estos dos derechos consiste en la existencia de un proveedor de servicios que conserve los datos de identidad de los clientes y trasmita un seudónimo a la empresa.[30] Cuando un cliente se dirija al proveedor, para ejercer el derecho de acceso o el derecho a la portabilidad de los datos, éste enviará el seudónimo a la empresa para que dé acceso al cliente a sus datos. Conviene advertir, por otro lado, que no sólo el RGPD prevé un derecho de acceso a los datos personales, también el R.D. contempla el derecho de acceso del usuario de los datos. Así, cuando un usuario no sea el interesado y pretenda acceder a los datos personales generados por el uso de un producto conectado y de un servicio relacionado, deberá acreditar una de las justificaciones del art. 6 RGPD. Además, aunque el usuario pueda estar legitimado para procesar datos personales ex art. 6 RGPD, el titular de los datos, según se indica en el Considerando 8 del R.D., deberá anonimizarlos o, si ello fuera posible, transmitir únicamente los datos personales relativos al usuario.

Pues bien, el art. 17. 1, letra g) del R.D. incluye también la seudonimización entre las garantías adecuadas, aunque parece una posibilidad suplementaria o complementaria a la petición de anonimización. Cuando se regula el cumplimiento de las solicitudes de datos por parte del titular, se confirma la prevalencia de la anonimización para los supuestos de datos personales (art. 18.4 R.D.).[31] En definitiva, la seudonimización de los derechos de acceso y de portabilidad de los datos juega un papel residual frente a la anonimización y puede lograse adecuadamente mediante un proveedor de servicios. Dicho esto, la seudonimización prevalece cuando la solicitud provenga de un organismo público y se exija la publicación de datos personales. Como hecho curioso, se prevé una compensación al titular de los datos por los gastos de seudonimización (art. 20.2 R.D. y art. 15.1 a) y b) R.D.).[32] En definitiva, no incorporamos aquí ningún nuevo requisito para la seudonimización fuerte.

[30] COMITÉ EUROPEO DE PROTECCIÓN DE DATOS CEPD. *Guidelines 01/2025 on Pseudonymisation*. Bruxelas: European Data Protection Board, 2025. Anexo, caso 10.

[31] Véanse, también, el art. 15.1, letra a), sobre la necesidad excepcional de utilizar los datos por una emergencia pública y el art. 17.2, letra e) del R.D. sobre la solicitud en tales casos en forma seudonimizada.

[32] Sobre las compensaciones, véanse también el Considerando 75 y el art. 9 R.D.

5 Reutilización de los datos seudonimizados

En cambio, la reutilización de los datos seudonimizados, en cumplimiento de la gobernanza de datos, va a requerir la seudonimización más segura.[33] Tanto los servicios de intermediación de datos, como los organismos competentes públicos proveerán asistencia técnica a los titulares de los datos, incluida la seudonimización y la anonimización. De acuerdo con el artículo 7.1 del Reglamento Europeo de Gobernanza de Datos (en adelante, RGD), cada Estado miembro de la Unión Europea designará un organismo competente para prestar asistencia técnica a los organismos públicos que concedan o denieguen acceso para la reutilización de los datos confidenciales, protegidos por la propiedad intelectual o los datos personales.[34] Así, siguiendo al art. 7.4, letra c) del RGD, la asistencia incluirá el apoyo técnico para la seudonimización.

En cuanto a los servicios de intermediación de datos, el artículo 12, letra e) RGD contempla la oferta de herramientas y servicios, entre otras la anonimización y la seudonimización, previa solicitud o aprobación expresa del titular de los datos o del interesado y siempre que no se utilicen para otros fines.[35] Pues bien, en la prestación de intermediación de datos, la relación entre el titular de los datos, el mediador y el usuario de datos, puede emplearse una seudonimización mediante cifrado polimórfico, mencionado anteriormente (PEP).[36] Así, aunque en los Espacios de salud cada paciente tiene un identificador único, el mediador podría transformarlo luego en diferentes seudónimos según el usuario y la intención de compartir los datos seudonimizados. Para cada receptor, el mediador genera un nuevo seudónimo y por consiguiente no puede vincularse.

La seudonimización también sería una de las posibles soluciones para aquellos tratamientos en los cuales no es posible anonimizar los datos. Esta circunstancia debe estar prevista en la evaluación de impacto de protección de datos (EIPD) y el responsable debe mostrar que se supera el criterio de la proporcionalidad de la medida. Para ello, los datos se podrían transferir al espacio de datos del mediador, que trasladaría los datos a un entorno de tratamiento seguro aplicando seudonimización, entre otras posibles estrategias. Evidentemente, cualquier extracción de datos del ámbito de titular de los datos deberá garantizar la minimización de los datos. Por otro lado, el Reglamento de Gobernanza de Datos también prevé,

---

[33] ORTIZ DE URBINA CRIADO, Marta et al. Realidad y Retos de la Reutilización de Datos Abiertos. *Working Papers on Operations Management*, v. 16, 2025. DOI: https://doi.org/10.4995/wpom.23472.

[34] Art. 7.1 del Reglamento (UE) 2022/868 del Parlamento Europeo y del Consejo, de 30 de mayo de 2022, relativo a la gobernanza europea de datos y por el que se modifica el Reglamento (UE) 2018/1724 (Reglamento de Gobernanza de Datos, RGD).

[35] Art. 12, letra e) del RGD: "Condiciones para la prestación de servicios de intermediación de datos".

[36] Seguimos aquí el ejemplo de la Agencia Española de Protección de Datos. *Aproximación a los Espacios de datos desde la perspectiva del RGPD*. [S.l.]: AEPD, 2023. p. 59-62.

en su Considerando 15, que la reutilización de los datos seudonimizados puede llevar a una re-identificación. Si ello se produjese, entonces debería realizarse una notificación por brecha de seguridad de los datos personales.

La separación física entre titular de los datos y mediador, y la previsión de un espacio ad-hoc para extraer la información a compartir, son garantías generales que combinadas con el uso de la seudonimización pueden ayudar a proteger los datos. Sin embargo, la existencia de guardianes de acceso, como los que dan servicio de computación en nube, puede comprometer la eficacia de tales medidas.[37] Así, las separaciones de datos se diluyen si todos los intervinientes seleccionan al mismo guardián de acceso como encargado de tratamiento. Como vemos, el contexto de la computación en nube afecta a la seudonimización fuerte. De manera general, la IA generativa puede limitar o incluso anular las garantías de los seudónimos como vamos a ver a continuación.

6 Inteligencia artificial y seudónimos

En un artículo pre-publicado en arXiv.org el 26 de febrero de 2026, investigadores del ETH Zurich llegan a la conclusión que los seudónimos no ofrecen una protección significativa en las redes sociales.[38] Así, el uso de LLM IA, es decir IA generativa, por parte de un atacante con recursos moderados es suficiente para identificar a los usuarios de los seudónimos. Esto no hace sino confirmar que el contexto es clave y que las evaluaciones de impacto deben incorporar el posible uso de una IA generativa por parte de un atacante con recursos moderados.

Por otro lado, existen numerosas herramientas para seudonimizar datos médicos.[39] Pese a ello, la desidentificación que deberían aportar los seudónimos sobre los datos médicos que luego se ofrecen en abierto no es efectiva. Algunos autores hablan, en este sentido, de una disolución de la diferencia entre los datos identificables y los no-identificables. Por ello, se ha acuñado el concepto de seudo-reidentificación, es decir la reidentificación de seudónimos mediante IA.[40] Las posibles soluciones del Proyecto AI.READI han sido la verificación de identidad, la firma de licencias con la declaración expresa de la intención de uso, así como

[37] Agencia Española de Protección de Datos. *Aproximación a los Espacios de datos desde la perspectiva del RGPD*. [S.l.]: AEPD, 2023. p. 81-85.

[38] LERMEN, Simon Lermens et al. *Large-scale online deanonymization with LLMs*. Disponible en: https://arxiv.org/abs/2602.16800. Acceso el: 25 feb. 2026.

[39] ATTIEH, Hammam Abu et al. Pseudonymization tools for medical research: a systematic review. *BMC Medical Informatics and Decision Making*, v. 25, art. 128, 2025. DOI: https://doi.org/10.1186/s12911-025-02958-0.

[40] HALLAJ, Shahin et al. Navigating open data sharing and privacy in the age of clinical AI research: from reidentification to pseudo-reidentification. *eClinicalMedecine*, v. 91, art. 103729. 2026. DOI: https://doi.org/10.1016/j.eclinm.2025.103729.

la trazabilidad posterior mediante marcas de agua.[41] Como vemos, se busca identificar y comprometer al usuario que accede a los datos abiertos para poder cotejar posteriormente su actividad, con la garantía de poder probar un hipotético mal uso de estos.

7 Conclusiones

Nos proponíamos en este trabajo valorar los requisitos de la seudonimización fuerte y el reto de la re-identificación mediante inteligencia artificial. Tanto el CEPD como ENISA coinciden en enmarcar el uso de la seudonimización fuerte en una evaluación de riesgo de protección de datos que tenga en cuenta el contexto y las características del tratamiento de datos, que el primero llama dominio de la seudonimización.[42] Queda pendiente, con todo, el reto mayúsculo de unas futuras Recomendaciones sobre anonimización, que deberían sustituir el trabajo del Grupo 29 de 2014. Es fácil ver porqué cuesta tanto: lo anónimo define en negativo el ámbito de la protección de datos. La tendencia que sugiere el dominio de la seudonimización anticipa, al menos parcialmente, una definición más funcional del dato personal.[43] En este sentido, lo identificable cobra importancia sobre lo identificado, lo cual supone una aplicación prevalente de la aproximación basada en el riesgo.[44] Ya no es suficiente con la individualización (*distinguishability*), ahora es cada vez más necesario evaluar también la disponibilidad de los datos (*availability*).[45] Para ello, la información del contexto y los controles serán ahora

41 HALLAJ, Shahin et al. AI-READI Consortium. Navigating open data sharing and privacy in the age of clinical AI research: from reidentification to pseudo-reidentification. *eClinicalMedicine*, v. 91, art. 103729. 2026. DOI: 10.1016/j.eclinm.2025.103729.

42 AGENCIA DE LA UNIÓN EUROPEA PARA LA CIBERSEGURIDAD (ENISA). *Data Pseudonymisation: Advanced Techniques & Use Cases: technical analysis of cybersecurity measures in data protection and privacy.* [S.l.]: ENISA, 2021. p.6. Conclusions and Recommendations.

43 STALLA-BOURDILLON, Sophie. Identifiability, as a Data Risk: Is a Uniform Approach to Anonymisation About to Emerge in the EU? *European Journal of Risk Regulation*, v. 16, n. 4, p.1456-1474, 2025. DOI: https://doi.org/10.1017/err.2025.16. El CEPD también endurece la exigencia de la prueba de anonimización al incluir no sólo la probabilidad de extracción directa de datos personales, sino también la probabilidad de obtener, voluntaria o involuntariamente los datos personales a partir de cualquier medio razonable que pueda usar el encargado o un tercero. Para poder realizar este análisis, deberá revisarse la documentación relativa al modelo de anonimización que obre en poder del encargado y se establece una lista de métodos a seguir (CEPD, *Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models*, adoptado el 17 de diciembre de 2024).

44 Solove lleva esta postura a sus últimas consecuencias cuando sostiene la conveniencia de abandonar las categorías especiales de datos personales del art. 9 RGPD por una perspectiva basada en el riesgo y el daño. Según él, las distinciones basadas en el tipo de dato no son relevantes en un mundo de inferencias. En este sentido, todos los datos personales acabarán siendo potencialmente sensibles. Si nos basamos en el perjuicio y el riesgo, en cambio, podremos proteger proporcionalmente al riesgo potencial o al daño que se produzca (SOLOVE, Daniel J. Data is what data does: Regulating Based on Harm and Risk instead of Sensitive Data. *Northwestern University Law Review*, v. 118, n. 4, p.1081-1137, 2024).

45 STALLA-BOURDILLON, Sophie. Identifiability, as a Data Risk: Is a Uniform Approach to Anonymisation About to Emerge in the EU? *European Journal of Risk Regulation*, v. 16, n. 4, 2025. p. 1458. La autora menciona concretamente los casos del TJUE Breyer (Patrick Breyer v Bundesrepublik Deutschland (2016)

determinantes en el intercambio de datos. La discusión sigue abierta, sin embargo, sobre qué metodología utilizar para llevar a cabo una evaluación de riesgo cada vez más global. Tenemos algunas indicaciones provenientes del informe del CEPD 28/2024, sobre modelos de inteligencia artificial:[46] la anonimización requiere hacer frente a la individualización, la conexión y la inferencia; además, si no se puede proteger una de las tres, puede realizarse una evaluación global de los riesgos de re-identificación por parte de terceros no previstos.[47]

En cualquier caso, a la espera de las Recomendaciones del CEPD sobre anonimización, las conclusiones del presente estudio confirman que el uso de técnicas seudonimizadoras avanzadas no es suficiente si se contempla como una solución aislada; en su lugar, conviene plantear opciones organizativas y arquitecturas institucionales alineadas con ella. Hemos podido ver los retos que plantean, al respecto, los centros de gestión de datos y la IA generativa. Por otro lado, la transferencia internacional de datos, así como las políticas de open data van a requerir un uso creciente de la seudonimización fuerte. Empiezan a aparecer buenas prácticas; ahora es necesaria una difusión de éstas que permita ofrecer soluciones adaptadas a los múltiples dominios de seudonimización que plantea la más reciente regulación europea.

Referencias bibliográficas

ARIAS POU, María. Definiciones a efectos del Reglamento General de Protección de Datos. In: PIÑAR MAÑAS, José Luis (dir.); ÁLVAREZ CARO, María; RECIO GAYO, Miguel (coords.). *Reglamento General de Protección de Datos: hacia un nuevo modelo europeo de privacidad.* Madrid: Editorial Reus, 2016. p. 115-134.

ATTIEH, Hammam Abu et al. Pseudonymization tools for medical research: a systematic review. *BMC Medical Informatics and Decision Making*, Londres, v. 25, art. 128, 2025. DOI: https://doi.org/10.1186/s12911-025-02958-0.

AGENCIA DE LA UNIÓN EUROPEA PARA LA CIBERSEGURIDAD (ENISA). *Ingeniería de compartición de datos personales: casos de uso y tecnologías emergentes.* Versión 1. [S.l.]: ENISA, 2023.

AGENCIA DE LA UNIÓN EUROPEA PARA LA CIBERSEGURIDAD (ENISA). *La adopción de técnicas de seudonimización: el caso del sector sanitario.* [S.l.]: ENISA, 2022.

AGENCIA DE LA UNIÓN EUROPEA PARA LA CIBERSEGURIDAD (ENISA). *Data Pseudonymisation: Advanced Techniques & Use Cases: technical analysis of cybersecurity measures in data protection and privacy.* [S.l.]: ENISA, 2021.

CLI:EU:C:2016:779), Scania (Gesamtverband Autoteile-Handel eV v Scania CV AB [2023] CJEU C-319/22, ECLI:EU:C:2023:837), IAB Europe (C-604/22 IAB Europe [2024] CJEU C-604/22, ECLI:EU:C:2024:214.) y el caso SRB cuya apelación todavía está pendiente de resolución en el momento de publicar este trabajo (Single Resolution Board (SRB) v European Data Protection Supervisor (EDPS) [2023] General Court Case T-557/20).

46 CEPD, *Opinion 28/2024 on Certain Data Protection Aspects Related to the Processing of Personal Data in the Context of AI Models*. Adoptado el 17 dec. 2024.

47 Esta posibilidad de anonimización basada en el riesgo no se encuentra en el Dictamen del Grupo de Trabajo del artículo 29. *Dictamen 05/2014 sobre técnicas de anonimización* (WP 136). Adoptado el 20 de junio de 2007.

AGENCIA DE LA UNIÓN EUROPEA PARA LA CIBERSEGURIDAD (ENISA). *Pseudonymisation techniques and best practices: recommendations on shaping technology according to data protection and privacy provisions.* [S.l.]: ENISA, 2019.

AGENCIA DE LA UNIÓN EUROPEA PARA LA CIBERSEGURIDAD (ENISA). *Recommendations on shaping technology according to GDPR provisions: an overview on data pseudonymisation*. [S.l.]: ENISA, 2018.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD). *Aproximación a los Espacios de datos desde la perspectiva del RGPD.* [S.l.]: AEPD, 2023.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD). *Orientaciones para la validación de sistemas criptográficos en la protección de datos.* [S.l.]: AEPD, 2023.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS; SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS (AEPD/EDPS). *Introducción al hash como técnica de seudonimización de datos personales.* [S.l.]: AEPD/EDPS, 2019.

COMITÉ EUROPEO DE PROTECCIÓN DE DATOS. *Guidelines 01/2025 on pseudonymisation.* Bruxelas: European Data Protection Board, 2025. Adoptado el 16 ene. 2025.

CONTE, Raffaelle et al. Privacy-by-design and minimization within a small electronic health record: the Health360 case study. *Applied Sciences*, v. 12, n. 17, art. 8441, 2022. DOI: https://doi.org/10.3390/app12178441.

DONADIEU, Gwenaëlle. Le RGPD et la protection de la vie privée face à l'essor des objets connectés. *Tic & société*, v. 15, n. 2-3, p. 217-239, 2022. DOI: https://doi.org/10.4000/ticetsociete.6720.

European Medicines Agency. *External guidance on the implementation of the European Medicines Agency policy on the publication of clinical data for medicinal products for human use*, de 15 de octubre de 2018, EMA/90915/2016, versión 1.4, p. 41.

FINCK, Michele; BIEGA, Asia J. Reviving purpose limitation and data minimisation in data-driven systems. *Technology and Regulation,* p. 44-61, 2021. DOI: https://doi.org/10.71265/z7r0t122.

GRUPO DE TRABAJO DEL ARTÍCULO 29. *Dictamen 4/2007: sobre el concepto de datos personales* (WP 136). Adoptado el 20 de junio de 2007.

HALLAJ, Shahin et al. Navigating open data sharing and privacy in the age of clinical AI research: from reidentification to pseudo-reidentification. *eClinicalMedicine*, v. 91, art. 103729, 2026. DOI: https://doi.org/10.1016/j.eclinm.2025.103729.

HALLAJ, Shahin et al. *Open Data Sharing in Clinical Research and Participants Privacy: Challenges and Opportunities in the Era of Artificial Intelligence*. 2025. Disponible en: https://arxiv.org/abs/2508.01140. Acceso el: 25 feb. 2026.

LERMEN, Simon et al. *Large-scale online deanonymization with LLMs.* 2026. Disponible en: https://arxiv.org/abs/2602.16800. Acceso el: 25 feb. 2026.

NAEF, Tobias. *Data Protection without Data Protectionism: The Right to Protection of Personal Data and Data Transfers in EU Law and International Trade Law*. Zurich: Springer, 2023. DOI: https://doi.org/10.1007/978-3-031-19893-9.

ORTIZ DE ORBINA CRIADO, Marta et al. Realidad y Retos de la Reutilización de Datos Abiertos. *Working Papers on Operations Management,* v. 16, 2025. DOI: https://doi.org/10.4995/wpom.23472.

PARK, Hyun A. The DtMin Protocol: Implementing Data Minimization Principles in Medical Information Sharing. *Electronics,* Basel, v. 14, n. 8, art. 1501, 2025. DOI: https://doi.org/10.3390/electronics14081501.

PUYOL MONTERO, Francisco Javier. Los principios del derecho a la protección de datos. In: PIÑAR MAÑAS, José Luis (dir.); ÁLVAREZ CARO, María; RECIO GAYO, Miguel (coords.). *Reglamento General de Protección de Datos*: *hacia un nuevo modelo europeo de privacidad.* Madrid: Editorial Reus, 2016. p. 135-150.

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*, Barcelona, v. 2, p. 525-551, 2024.

ROIG BATALLA, Antoni. *Las garantías frente a las decisiones automatizadas: del Reglamento General de Protección de Datos a la gobernanza algorítmica.* Barcelona: Bosch, 2020. DOI: https://doi.org/10.2307/j.ctv1dv0v54.

ROIG BATALLA, Antoni. *La expectativa razonable de privacidad: orígenes y recepción jurisprudencial en España*. Barcelona: Bosch, 2024.

SOLOVE, Daniel J. Data Is What Data Does: Regulating Based on Harm and Risk instead of Sensitive Data. *Northwestern University Law Review*, v. 118, n. 4, p. 1081-1137, 2024.

STALLA-BOURDILLON, Sophie. Identifiability, as a Data Risk: is a Uniform Approach to Anonymisation About to Emerge in the EU? *European Journal of Risk Regulation*, v. 16, n. 4, p. 1456-1474, 2025. DOI: https://doi.org/10.1017/err.2025.16.

TERWANGNE, Cécile de; BYGRAVE, Lee A. Article 5: principles relating to processing personal data. In: KUNER, Christopher; BYGRAVE, Lee A.; DOCKSEY, Christopher (dirs.). *The European Union General Data Protection Regulation: a commentary.* Oxford: Oxford University Press, 2020. p. 309-320. DOI: https://doi.org/10.1093/oso/9780198826491.003.0034.

TOSONI, Luca. Article 4(5): Pseudonymisation. In: KUNER, Christopher; BYGRAVE, Lee A.; DOCKSEY, Christopher (eds.). *The European Union General Data Protection Regulation (GDPR): a commentary.* Oxford: Oxford University Press, 2020. DOI: https://doi.org/10.1093/oso/9780198 826491.001.0001.

VON GRAFESTEIN, Max. *The Principle of Purpose Limitation in Data Protection Laws: the Risk-based Approach, Principles, and Private Standards as Elements for Regulating Innovation.* Baden-Baden: Nomos, 2018.

Informação bibliográfica deste texto, conforme a NBR 6023:2025 da Associação Brasileira de Normas Técnicas (ABNT):

ROIG BATALLA, Antoni. La protección de datos mediante la seudonimización fuerte. *International Journal of Digital Law*, Belo Horizonte, v. 7, e706, 2026. DOI: 10.47975/ijdl.v7.1348.

Informações adicionais

Additional information