PANELFIT

PARTICIPATORY APPROACHES TO A NEW ETHICAL AND LEGAL FRAMEWORK FOR ICT

Directrices sobre cuestiones éticas y jurídicas de la protección de datos en la investigación e innovación en materia de TIC

REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS (RGPD) – CONCEPTOS PRINCIPALES

Este proyecto ha sido financiado por el programa de investigación e innovación Horizonte 2020 de la Unión Europea mediante el acuerdo de subvención nº 788039. Este documento refleja únicamente las opiniones de los autores, y la Agencia no se hace responsable del uso que pueda hacerse de la información contenida en él.

2 Conceptos principales

2.1 Datos personales

Simona Sobotovicova (UPV/EHU)

Esta parte de las Directrices fue revisada por Daniel Jove Villares, Universidade Da Coruna, España

Esta parte de las Directrices ha sido revisada y validada por Marko Sijan, Asesor Superior Especialista, (HR DPA)

2.1.1 El concepto de datos personales

Por datos personales se entiende cualquier información relativa a una persona física identificada o identificable ("sujeto de los datos"). La definición de datos personales según el RGPD añade que una persona física identificable es aquella que puede ser identificada, directa o indirectamente, en particular por referencia a un identificador como un nombre, un número de identificación, datos de localización, un identificador en línea o a uno o más factores específicos de la identidad física, fisiológica, genética, mental, económica, cultural o social de dicha persona[54] física. No cabe duda de que el objetivo de las normas contenidas en el RGPD es proteger los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la intimidad, en relación con el tratamiento de los datos personales. Sin embargo, debido a la amplia definición de datos personales establecida en el RGPD, el Grupo de Trabajo de Protección de Datos del artículo 29, las autoridades nacionales de control de la protección de datos y la jurisprudencia del Tribunal de Justicia de las Comunidades Europeas (en adelante, TJCE) respaldan la definición de datos personales.

El análisis del concepto de datos personales realizado por el Grupo de Trabajo de Protección de Datos del Artículo 29 en el Dictamen 4/2007 se ha basado en los siguientes cuatro "componentes" principales que pueden distinguirse en la definición de "datos[55] personales":

- *"Cualquier información"* - Este término indica claramente la voluntad del legislador de diseñar un concepto amplio de datos personales. Esta redacción exige una interpretación amplia. Abarca información "objetiva", como la presencia de una determinada sustancia en la sangre. También incluye información "subjetiva", opiniones o valoraciones. Además, para que una información sea un "dato personal", no es necesario que sea verdadera o esté probada.

---

[54] Artículo 4(1) del RGPD.

55 *Véase*, Grupo de Trabajo de Protección de Datos del Artículo 29: Dictamen 4/2007 sobre el concepto de datos personales. Adoptado el 20 de junio, 01248/07/ES WP 136, pp.9-12, 21. Disponible en: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf

Hay que decir que, el concepto de datos personales incluye una gama muy amplia de información, "no sólo objetiva, sino también subjetiva", en forma de opiniones y valoraciones, siempre que se "relacione" con el interesado[56].

- *"Relativo a"* - En términos generales, se puede considerar que la información se "relaciona" con un individuo cuando es sobre ese individuo. Cabe señalar que, para considerar que los datos se "relacionan" con un individuo, debe estar presente un elemento de "contenido" o un elemento de "finalidad" o un elemento de "resultado". Estos tres elementos (contenido, finalidad, resultado) deben considerarse como condiciones alternativas, y no como acumulativas, por lo que basta con la presencia de uno de estos elementos para considerar que se "relacionan" con un individuo.

En palabras del TJCE, los criterios de contenido, finalidad o efecto actúan como parámetro para clasificar determinada información como datos personales. Si el contenido, la finalidad o el efecto están vinculados a una persona concreta, entonces la información es un dato personal. La utilización de uno de estos criterios es suficiente para que exista la posibilidad de clasificar una determinada información como dato personal[57].

- *"Una persona identificada o identificable"* - En términos generales, una persona física puede considerarse "identificada" cuando, dentro de un grupo de personas, se "distingue" de todos los demás miembros del grupo. En consecuencia, la persona física es "identificable" cuando, aunque la persona no haya sido identificada todavía, es posible hacerlo (ése es el significado del sufijo "-able").

El RGPD menciona esos "identificadores" en la definición de "datos personales" del artículo 4, apartado 1, mencionada anteriormente. Además, para determinar si una persona física es identificable, deben tenerse en cuenta todos los medios que puedan utilizarse razonablemente, como la identificación, ya sea por el responsable del tratamiento o por otra persona, para identificar a la persona física directa o indirectamente[58]. Sin embargo, la cuestión de si la persona es "identificable" sigue siendo el centro de atención de los recientes debates[59] académicos.

- "Persona física" - La protección se aplica a las personas físicas, es decir, a los seres humanos. El derecho a la protección de los datos personales es, en ese sentido, un derecho universal que no se limita a los nacionales o residentes en un determinado país.

El RGPD establece que las personas físicas pueden estar asociadas a identificadores en línea proporcionados por sus dispositivos, aplicaciones, herramientas y protocolos, como

---

[56] Sentencia del Tribunal de Justicia de la Unión Europea (Sala Segunda), asunto C-43 4/16, *Peter Nowak contra el Comisario de Protección de Datos*, 20 de diciembre de 2017, §34.

[57] Sentencia del Tribunal de Justicia de la Unión Europea (Sala Segunda), asunto C-43 4/16, *Peter Nowak contra el Comisario de Protección de Datos*, 20 de diciembre de 2017, §35.

[58] Considerando (26) RGPD.

[59] *Véase*, por ejemplo, Purtova, N. (2018). La ley del todo. Concepto amplio de datos personales y futuro de la ley de protección de datos de la UE. *Derecho, innovación y tecnología*. DOI:https://doi.org/10.1080/17579961.2018.1452176.

direcciones de protocolo de Internet, identificadores de cookies u otros identificadores como etiquetas de identificación por radiofrecuencia. Esto puede dejar rastros que, en particular cuando se combinan con identificadores únicos y otra información recibida por los servidores, pueden utilizarse para crear perfiles de las personas físicas e identificarlas[60]. Además, los principios y las normas de protección de las personas físicas en relación con el tratamiento de sus datos personales deben respetar, cualquiera que sea su nacionalidad o residencia, sus derechos y libertades fundamentales, en particular su derecho a la protección de los datos personales. El presente Reglamento tiene por objeto contribuir a la realización de un espacio de libertad, seguridad y justicia y de una unión económica, al progreso económico y social, al refuerzo y a la convergencia de las economías dentro del mercado interior, así como al bienestar de las personas físicas[61].

El Grupo de Trabajo de Protección de Datos del Artículo 29 afirma que estos cuatro elementos previstos en la primera frase de la definición de datos personales *(cualquier información relativa a una persona física identificada o identificable)* están estrechamente relacionados y se alimentan mutuamente, pero juntos determinan si una información debe considerarse "datos personales".

2.1.2 ¿Qué información puede considerarse como datos personales?

Las Autoridades Nacionales de Supervisión de la Protección de Datos y la jurisprudencia del TJCE desempeñan un papel esencial a la hora de interpretar las disposiciones legales y ofrecer orientaciones concretas a los responsables del tratamiento y a los interesados, respaldando una definición de datos personales lo suficientemente amplia. La definición de los datos personales es un elemento central para la aplicación e interpretación de las normas de protección de datos que tienen un profundo impacto en una serie de cuestiones y temas importantes. Teniendo en cuenta el formato o el soporte en el que está contenida esa información, el concepto de datos personales incluye la información disponible en cualquier forma, ya sea alfabética, numérica, gráfica, fotográfica o acústica, por ejemplo[62]. El TJCE establece una clasificación de la información como datos personales en diferentes sentencias. En este sentido, el término datos personales abarca sin duda el nombre de una persona junto con sus coordenadas telefónicas o la información sobre sus condiciones de trabajo o aficiones. También la información contenida en texto libre en un documento electrónico puede calificarse de datos personales, siempre que se cumplan los demás criterios de la definición de datos personales. El correo electrónico, por ejemplo, contendrá "datos personales". El TJCE se ha pronunciado en este sentido al considerar que "referirse, en una página de Internet, a varias personas e identificarlas por su nombre o por otros medios, por ejemplo, dando su número de teléfono o información sobre sus condiciones de trabajo y aficiones, constituye un tratamiento de datos personales [...][63].

---

60 Considerando (30) RGPD.

61 Considerando (2) RGPD.

62 Grupo de Trabajo de Protección de Datos del Artículo 29: Dictamen 4/2007 sobre el concepto de datos personales. Adoptado el 20 de junio, 01248/07/ES WP 136, p.7. Disponible en: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf

63 Sentencia del Tribunal de Justicia Europeo, C-101/2001, *Lindqvist*, §27, 06.11.2003.

El 20 de diciembre de 2017 el TJUE dictó su sentencia sobre el "caso *Nowak*" [64]establece la calificación de las respuestas y comentarios subjetivos del examinador dentro de las respuestas escritas presentadas por un candidato en un examen profesional como datos personales, estableciendo una serie de criterios que permiten entender qué datos son de carácter personal[65]. La sentencia aborda la posible aplicación del RGPD para constituir datos personales[66]. Cabe destacar que, la calificación de estos datos como personales conlleva, para el candidato, la posibilidad de utilizar sus derechos de acceso, rectificación y oposición. En este sentido, la calificación como datos personales proporciona el derecho de acceso, pero también las demás facultades que se otorgan al titular de este tipo de datos, que son: los derechos de rectificación, supresión y oposición, así como todas las garantías recogidas en la legislación[67] de protección de datos.

La sentencia también analiza la aplicabilidad del derecho de acceso a datos con más de un titular e intereses contrapuestos (en este caso el examinador y el candidato). El TJCE se reafirma en la idea de que, el hecho de que la información esté en manos de una o varias personas es irrelevante respecto a su calificación como datos personales. La atribución de la condición de datos personales no proviene de este hecho, sino de la propia naturaleza de la información. En cuanto a la definición de datos personales, el TJCE añade otra característica a ésta: la pluralidad de afectados, o la posibilidad de que una información pueda ser un dato personal de más de un interesado[68].

Debido a la calificación de una información como dato personal, en el [69]*caso YS y otros*, se considera que el análisis jurídico de una minuta elaborada en el marco de una solicitud de permiso de residencia, no es un dato personal ya que se refiere a "información sobre la evaluación y aplicación por la autoridad competente de la ley a la situación del solicitante". Esta interpretación hizo que, en el caso *YS y otros*, no se reconociera el derecho de acceso a esa información, al considerar que dicho acceso se basaría en un derecho de acceso a los documentos públicos que no está contemplado en la legislación del RGPD[70]. Sin embargo, si el análisis hubiera incluido alguna evaluación del sujeto, o que pudiera tener un esfuerzo sobre él, entonces se consideraría como datos personales que, como tales, estarían sujetos al RGPD [71].

---

64 Sentencia del Tribunal de Justicia de la Unión Europea (Sala Segunda), asunto C-43 4/16, *Peter Nowak contra el Comisario de Protección de Datos*, 20 de diciembre de 2017.

65 Jove, D. (2019). Peter Nowak contra el comisario de protección de datos: Posibles secuelas en relación con las anotaciones subjetivas en las historias clínicas. *Revista Europea de Derecho de la Protección de Datos*, volumen 5, número 2, p. 175. DOI: https://doi.org/10.21552/edpl/2019/2/7

66 Sentencia del Tribunal de Justicia de la Unión Europea (Sala Segunda), asunto C-43 4/16, *Peter Nowak contra el Comisario de Protección de Datos*, 20 de diciembre de 2017, §27.

67 Jove, D. (2019). Peter Nowak contra el comisario de protección de datos: Posibles secuelas en relación con las anotaciones subjetivas en las historias clínicas. *Revista europea de derecho de la protección de datos*, volumen 5, número 2, p. 177. DOI: https://doi.org/10.21552/edpl/2019/2/7

68 *Ibídem*, p. 176, 178.

69 Sentencia del Tribunal de Justicia, asuntos acumulados C-141/12 y C-372/12, *YS y otros*, 17 de julio de 2014.

70 Sentencia del Tribunal de Justicia, asuntos acumulados C-141/12 y C-372/12, *YS y otros*, 17 de julio de 2014, §40.

71 Jove, D. (2019). Peter Nowak contra el Comisionado de Protección de Datos: Posibles secuelas en relación con las anotaciones subjetivas en las historias clínicas. *Revista Europea de Derecho de la Protección de Datos*, volumen 5, número 2, p. 179. DOI: https://doi.org/10.21552/edpl/2019/2/7

Podría afirmarse que la definición del RGPD, tal como recuerda el TJCE, se basa en una definición amplia de los datos personales que refleja la intención del legislador de asignar un amplio alcance al concepto, abarcando la información subjetiva y objetiva del interesado. Dado que la clasificación de la información como datos personales la sitúa en el ámbito de la arquitectura de protección de los derechos fundamentales de la UE, también establece tanto los derechos de los interesados como las circunstancias en las que puede disminuirse el nivel de protección debido a objetivos[72] justificables.

2.2 Procesamiento de datos

Iñigo de Miguel Beriain (UPV/EHU)

Esta parte de la Guía fue revisada por Daniel Jove Villares, Universidade Da Coruna, España

Esta parte de las Directrices ha sido revisada y validada por Marko Sijan, Asesor Superior Especialista, (HR DPA)

2.2.1 Definición

Según el apartado 2 del artículo 4 del RGPD, se entiende por tratamiento "cualquier operación o conjunto de operaciones, efectuadas o no por medios automatizados, relativas a datos personales o a conjuntos de datos personales, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación, cotejo o interconexión, limitación, supresión o destrucción".

Por lo tanto, el concepto de tratamiento es amplio. Abarca una amplia gama de operaciones realizadas con datos personales, incluso por medios manuales o automatizados, si forma parte de un sistema de archivo estructurado, es decir, un conjunto estructurado de datos personales que son accesibles según criterios específicos, ya sea centralizado, descentralizado o disperso sobre una base funcional o geográfica (art. 4(6)).

Evidentemente, la lista incluida en el apartado 2 del artículo 4 no es exhaustiva, lo que significa que otras operaciones con datos personales que se ajustan a la definición general también deberían considerarse tratamiento con arreglo al RGPD. Algunos ejemplos de tratamiento son: la gestión del personal y la administración de las nóminas; el acceso/consulta de una base de datos de contactos que contenga datos personales; el envío de correos electrónicos promocionales; la destrucción de documentos que contengan datos personales; la

72 Podstawa, K. (2018). Peter Nowak Comisario de Protección de Datos: Puedes acceder al guión de tu examen, porque son datos personales. *Revista europea de derecho de la protección de datos (EDPL),* 4(2), pp. 254, 256. DOI: https://doi.org/10.21552/edpl/2018/2/17.

publicación/puesta de una foto de una persona en un sitio web; el almacenamiento de direcciones IP o direcciones MAC; la grabación de vídeo (CCTV), etc. [73]

2.2.2 El tratamiento como concepto clave en el RGPD

El tratamiento es un elemento esencial en términos de derechos de protección de datos. Lo que realmente regula el RGPD no son los datos en sí, sino el tratamiento de los datos personales. Este uso de los datos desencadena la aplicación de la normativa de protección de datos. De hecho, el artículo 1.1 del RGPD establece que "El presente Reglamento establece normas relativas a la protección de las personas físicas en **lo que respecta al tratamiento de datos personales** y normas relativas a la libre circulación de datos personales."

Las circunstancias del tratamiento definen los elementos reglamentarios esenciales: la necesidad (o no) de encontrar un motivo para tratar los datos, si son de una categoría especial; la base de legitimación adecuada; si se trata de un tratamiento individual o de un tratamiento a gran escala; el nivel de riesgo específico; las garantías que deben aplicarse; etc. Cada tratamiento será, en definitiva, un hecho separado e independiente, con sus propias características y escala. De ahí que siempre haya que pensar que la normativa de protección de datos se aplica a cada uno de ellos.

2.3 Protección de datos por diseño y por defecto

Bud P. Bruegger (ULD)

Agradecimientos: El autor agradece la ayuda de Kirsten Bock en la interpretación jurídica, los comentarios y la revisión de Harald Zwingelberg y la detallada revisión y sugerencias de Hans Graux

Esta parte de las Directrices fue finalmente validada por Hans Graux, profesor invitado de derecho de las TIC y de protección de la intimidad en el Instituto de Derecho, Tecnología y Sociedad de Tilburg (TILT) y en la AP Hogeschool Antwerpen. Presidente del Vlaamse Toezichtscommissie (Comité Flamenco de Supervisión), que supervisa el cumplimiento de la protección de datos en los organismos del sector público flamenco

La presente sección pretende ofrecer a los profesionales una comprensión más detallada de cómo aplicar en la práctica los requisitos del artículo 25 del RGPD. 25 del RGPD sobre protección de datos por diseño y por defecto *(Data Protection by Design and Default o DPbDD)*.

La presente sección sobre Protección de datos por diseño y por defecto está estructurada como sigue:

73 Comisión Europea, *What constitutes data processing*, en: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-constitutes-data-processing_en.

En una primera subsección se analizan las directrices sobre el tema publicadas por el Comité Europeo de Protección de Datos (CEPD). Señala las diferencias con el enfoque adoptado aquí.

Una segunda subsección describe el alcance de las obligaciones derivadas del art. 25 del RGPD. Y lo que es más importante, aclara de qué manera afecta a los proveedores de tecnología.

Una tercera subsección analiza el Art. 25 del RGPD. Dado que el art. 25(1) obliga a los responsables del tratamiento a aplicar medidas tanto en el momento *de determinar los medios* como en el momento *del propio tratamiento*, se analiza el significado preciso de ***determinar los medios*** y del ***propio tratamiento***. Esto se basa en un análisis de lo que el RGPD establece sobre la estructura del tratamiento. El análisis del art. 25(1) también hace hincapié en el significado de la ***eficacia de las*** medidas. El análisis del art. 25(2) explica qué se entiende exactamente por el término ***incumplimiento*** y analiza las obligaciones del responsable del tratamiento.

Una cuarta subsección se centra en los procesos reales que implementan la protección de datos por diseño. En concreto, describe los procesos para aplicar la protección de datos por diseño y por defecto en las tres fases principales de *determinación de los fines*, *determinación de los medios* y el *propio tratamiento*. Estos procesos tienen como objetivo la aplicación sistemática de los principios de protección de datos en cada tarea de cada fase. El resultado es la identificación y aplicación de medidas técnicas y organizativas.

2.3.1 Directrices del Comité Europeo de Protección de Datos

El Comité Europeo de Protección de Datos (CEPD) ha publicado unas directrices sobre la protección de datos por diseño y por defecto[74]. Destaca la importancia de comprender y aplicar los **principios de protección de datos** (véase la sección "Principios principales" en la parte general de estas directrices) y de aplicar **los derechos del interesado** (véase la sección "Derechos del interesado" en la parte general de estas directrices).

La importancia de los principios de protección de datos se expresa, por ejemplo, en el apartado 61: "Los responsables del tratamiento deben aplicar los principios para lograr la protección de datos por diseño y por defecto *(Data Protection by Design and Default o DPbDD)*. Estos principios son: transparencia, legalidad, equidad, limitación de la finalidad, minimización de los datos, exactitud, limitación del almacenamiento, integridad y confidencialidad, y responsabilidad. Estos principios se describen en el artículo 5 y en el considerando 39 del RGPD. Para tener una comprensión completa de cómo aplicar la protección de datos por diseño y por defecto *(Data Protection by Design and Default o DPbDD)*, se destaca la importancia de entender el significado de cada uno de los principios".

La importancia de los derechos de los interesados se recoge en el apartado 63: "Si bien esta sección se centra en la aplicación de los principios, el responsable del tratamiento también debe aplicar formas adecuadas y eficaces de proteger los derechos de los interesados, también de acuerdo con el capítulo III del RGPD, cuando esto no sea ya un mandato de los propios principios."

La directriz del Comité Europeo de Protección de Datos (CEPD) dedica su sección 3 a la aplicación de los principios de protección de datos. Las directrices de PANELFIT van más

74 Comité Europeo de Protección de Datos, Directrices 4/2019 sobre la protección de datos del artículo 25 desde el diseño y por defecto, versión 2.0, adoptadas el 20 de octubre de 2020, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf (última visita: 30/11/2021).

allá al proporcionar una descripción más detallada de cada principio junto con muchos ejemplos de medidas técnicas y organizativas adecuadas para aplicar dichos principios.

Al igual que las directrices de Comité Europeo de Protección de Datos, también el siguiente texto analiza el significado del artículo 25 del RGPD. Sin embargo, el presente texto trata de proporcionar una orientación concreta adicional. Para ello, no sólo ofrece un análisis jurídico de las fases del tratamiento según el RGPD, sino que también proporciona un análisis técnico de las tareas necesarias para cada fase. En particular, esto se hace para *determinar los medios de tratamiento* y para *el propio tratamiento*. En cada una de las tareas que se identifican, se pueden aplicar los principios de protección de datos e identificar e implementar medidas técnicas y organizativas.

Una segunda diferencia importante entre el presente texto y las directrices de Comité Europeo de Protección de Datos es que el primero analiza el proceso real necesario para aplicar la protección de datos por diseño y por defecto en las distintas fases.

Una pequeña diferencia es que el presente texto profundiza en cómo los controladores pueden transmitir los requisitos a los productores de software y servicios. Sin embargo, el texto no entra en el mérito de la certificación; si esto fuera relevante para los lectores, se les remite a las directrices del Comité Europeo de Protección de Datos.

2.3.2 El alcance de la protección de datos por diseño y por defecto *(Data Protection by Design and Default o DPbDD)*

En esta sección se analiza cómo el RGPD contiene únicamente obligaciones para los responsables del tratamiento (y procesadores) y cómo esto puede influir indirectamente en los proveedores de tecnología.

La protección de datos desde el diseño puede considerarse como la consideración de la protección de datos no sólo en las *operaciones de tratamiento* que tienen lugar en la fase operativa, sino también en las fases anteriores de planificación y ejecución. En términos más generales, se podría considerar que la protección de datos desde el diseño es una metodología que tiene en cuenta la protección de datos en todas las fases del ciclo de vida de una *actividad*[75] de tratamiento, desde su concepción, pasando por su diseño e implementación, hasta su uso operativo y su desmantelamiento final.

El ciclo de vida completo suele implicar actividades por parte de otros actores además del responsable y el encargado del tratamiento. Lo más importante es que muchas decisiones que afectan a los aspectos de protección de datos de una actividad de tratamiento son tomadas por los proveedores de tecnología, que a menudo diseñan e implementan software y sistemas. Cuando los proveedores de tecnología invierten en el desarrollo de productos y servicios que luego se ofrecen en el mercado, también contribuyen a definir el *estado de la técnica* de un determinado tipo de tratamiento de datos personales.

En cambio, el RGPD establece obligaciones para los responsables y los encargados del tratamiento. Carece de cualquier obligación directa para los proveedores de tecnología. En su *dictamen preliminar sobre la privacidad desde el diseño*[76], el SEPD señala este hecho al afirmar lo siguiente: [77]

---

75 El término *actividad de tratamiento* se utiliza aquí en el sentido del Art. 30 *del* RGPD y 4(16)(b) del RGPD. En ambos casos, una actividad de *tratamiento* es la unidad básica de la empresa de un controlador que implica el tratamiento de datos personales.

76 El Supervisor Europeo de Protección de Datos (SEPD), Dictamen 5/2018, Dictamen preliminar sobre la privacidad desde el diseño, 31 de mayo de 2018, https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf (última visita 29/6/2020).

77 Páginas 7 y 8.

"Una grave limitación de las obligaciones del artículo 25 es que solo se aplican para imponer una obligación a los responsables del tratamiento y no a los desarrolladores de esos productos y tecnología utilizados para procesar datos personales. La obligación para los proveedores de productos y tecnología no está incluida en las disposiciones sustanciales del RGPD."

Dado que el RGPD en su conjunto, y el art. 25 en particular, expresan únicamente obligaciones para los responsables del tratamiento (y los encargados del mismo), el alcance de la presente sección se limita en consecuencia.

Aunque no existen obligaciones legales para los proveedores de tecnología, el art. 25 del RGPD les influye indirectamente. El considerando 78 del RGPD lo insinúa al afirmar lo siguiente[78] "Los principios de protección de datos por diseño y por defecto también deben tenerse en cuenta en el contexto de las licitaciones públicas". El modo en que se produce la influencia sobre los proveedores de tecnología se describe con más detalle en la siguiente sección.

El argumento se centra en el software creado por un proveedor de tecnología. Hay dos opciones para que un controlador pueda obtener dicho software:

- Como resultado de un desarrollo a medida, o
- Adquiriendo el software en el mercado.

En el primer caso, el diseño y el desarrollo del software es impulsado por el controlador y el proveedor de tecnología puede ser interno o externo; en el segundo caso, hay una multitud de controladores con necesidades similares que crean una demanda de mercado para ciertos tipos de software. El diseño y el desarrollo del software lo desencadena el proveedor de tecnología con el objetivo de lograr una posición competitiva en el mercado.

Los detalles técnicos inherentes al desarrollo de software suelen ser inaccesibles para los controladores y sus representantes. Por lo tanto, en ambos casos, la interacción entre los controladores y los proveedores de tecnología se limita a la comunicación sobre los requisitos. En concreto, el papel de los requisitos en los dos casos es el siguiente:

- En el caso del desarrollo a medida, los requisitos son la principal herramienta de los controladores para expresar los objetivos del proceso de desarrollo. Los requisitos también se utilizan para determinar si el proceso de desarrollo ha concluido con éxito. Esto ocurre durante las pruebas de aceptación.
- En el caso de los controladores que compran software, necesitan requisitos que les guíen en la selección del software adecuado entre la oferta del mercado. En el caso de las licitaciones, estos requisitos pueden comunicarse a los proveedores de tecnología para solicitar ofertas adecuadas a las necesidades; en el caso de la compra de software sin licitación, los controladores deben verificar si varias ofertas de software candidatas satisfacen los requisitos. En ambos casos, la validación de las ofertas en relación con los requisitos es un factor importante en la decisión de compra por parte del controlador.

Así, mientras que las obligaciones de los proveedores de tecnología están fuera del ámbito del art. 25, los responsables del tratamiento están obligados a determinar los requisitos de protección de datos adecuados y a asumir la plena responsabilidad del software que utilizan. La validación de los programas informáticos con respecto a los requisitos puede tener en cuenta el estado de la técnica y el coste de la aplicación (véase el artículo 25 del RGPD y el debate posterior). Sin embargo, la ausencia o el coste excesivo de un software adecuado en el mercado no puede considerarse una justificación válida para utilizar un software inadecuado.

78 Véase la frase 5.

2.3.3 Análisis del artículo 25. Protección de datos desde el punto de vista del diseño

La presente sección analiza la letra de la ley con el **objetivo** de encontrar **un enfoque estructurado y sistemático** para debatir las medidas que los responsables del tratamiento están obligados a aplicar por el Art. 25 del RGPD. La sistemática y la estructura resultantes se **utilizan en la sección 2.3.3.1 sobre las medidas**, que constituye la orientación más concreta para los profesionales.

Para facilitar la comprensión del texto, en el siguiente recuadro se definen dos términos de uso frecuente.

Definición: ***actividad de transformación***

El término *actividad de tratamiento* se utiliza aquí en el sentido del Art. 30 del RGPD y 4(16)(b) del RGPD. En ambos casos, una actividad de tratamiento es la unidad básica independiente de la empresa de un controlador que implica el tratamiento de datos personales. Una actividad de tratamiento se somete a un ciclo de vida que incluye la concepción, el diseño, la ejecución, el funcionamiento y el desmantelamiento.

Definición ***operación de tratamiento***

El término *operación de tratamiento* se refiere únicamente a la fase operativa de una *actividad de tratamiento* en la que un sistema de tratamiento funciona para tratar realmente los datos personales. Supone la ejecución de las *operaciones de tratamiento* tal y como se definen en el art. 4(2) del RGPD. Otros aspectos de las actividades de tratamiento, como la concepción y el diseño, no ejecutan dichas operaciones de tratamiento y, por tanto, no se consideran parte de las operaciones de tratamiento.

2.3.3.1 Visión general y principales obligaciones de los controladores

El art. 25 del RGPD incluye lo siguiente:

Art. 25(1):

Teniendo en cuenta [..], ***el responsable del tratamiento aplicará****, tanto en el momento de la determinación de los medios para el tratamiento como en el momento del propio tratamiento,* ***medidas técnicas y organizativas apropiadas*** *[...] destinadas a aplicar los principios de protección de datos [...] de manera eficaz y a integrar las garantías necesarias en el tratamiento [...].*

La principal obligación de los responsables del tratamiento establecida en el art. 25(1) del RGPD es, por tanto, que "***deberán*** *[.....]* ***aplicar las medidas técnicas y organizativas apropiadas*** *[...] destinadas* ***a aplicar los principios de protección de datos***" (véase la sección Principios fundamentales en la parte general de estas directrices).

A lo largo del RGPD[79], se afirma que la aplicación de medidas técnicas y organizativas es la forma de cumplir los principios de protección de datos. Esto implica que todo lo que hace un responsable del tratamiento en apoyo de los principios de protección de datos debe considerarse una medida. Por consiguiente, el **concepto de medida** debe **entenderse en un sentido muy amplio**. Esto significa que no se limita a los artefactos físicos (como los cortafuegos), o a acciones específicas (como la formación del personal). Más bien, debe abarcar también todas las consideraciones y decisiones necesarias para determinar los medios

79 Esto incluye, entre otros, los arts. 24, 25 y 32 del RGPD.

de tratamiento de manera que se ajusten a los principios y obligaciones de la protección de datos.

El art. 25(1) del RGPD también establece que estas medidas se aplicarán "de ***manera eficaz***". Por tanto, a continuación, se analizará la eficacia.

Además, el art. 25(1) establece que las medidas se aplican "***para integrar las garantías necesarias en el tratamiento***". En otras palabras, la aplicación de las medidas es la forma de lograr el objetivo de integrar las garantías necesarias en el tratamiento. Desde el punto de vista gramatical, esta interpretación resulta aún más clara cuando se amplía "para *integrar*" a su forma completa de "para *integrar*". El "para" excluye la interpretación de que, además de la aplicación de las *medidas*, también es necesaria *la integración de las garantías*.

Podría decirse que la esencia del art. 25(1) se encuentra en la redacción "*tanto en el momento* ***de la determinación de los medios*** *para el tratamiento como en el* ***momento del propio tratamiento"***. Esto significa que la aplicación de las medidas debe producirse en **dos períodos de tiempo distintos**. Por tanto, implica un **modelo de fases para una actividad de tratamiento**. Esto es compatible con la interpretación de la protección de datos desde el diseño, que considera la protección de datos en cada fase de una actividad de tratamiento. La interpretación jurídica de las fases de tratamiento contempladas en el art. 25(1) se ofrece en la siguiente subsección.

2.3.3.2 Las fases del tratamiento en el RGPD

El art. 25(1) del RGPD habla de dos fases en relación con una actividad de tratamiento, a saber, "**el momento *de la determinación de los medios* para el tratamiento**" y "**el momento del *propio tratamiento***". Es evidente que ambos *momentos* deben ser periodos de tiempo de cierta duración y no puntos en el tiempo. También es evidente que el momento de la determinación de los medios debe preceder al momento de la transformación propiamente dicha. Por lo tanto, llamamos a estos períodos de tiempo también ***fases***.

El art. 4(7) establece que, además de los medios, el responsable del tratamiento también "**determina los fines**". Evidentemente, esto también lleva tiempo y precede a la determinación de los medios. Parece útil incluir la determinación de los fines para completarla y en caso de que haya medidas que puedan aplicarse en esa fase.

En consecuencia, el RGPD implica el siguiente **modelo de fases de una actividad de tratamiento**:

- Fase 1: Determinación de los fines;
- Fase 2: Determinación de los medios;
- Fase 3: Procesamiento propiamente dicho.

Para entender mejor qué ocurre exactamente en cada fase, es necesario analizar con más detalle qué concepción tiene el RGPD de una operación de tratamiento.

2.3.3.3 Operaciones de tratamiento en el RGPD

A continuación, se analiza qué concepción tiene el RGPD de una operación de tratamiento.

El art. 5(1)(f) del RGPD establece la necesidad de "protección contra el tratamiento no autorizado"... Esto implica que el tratamiento ordinario debe ser **autorizado**. Del contexto también se desprende que dicha autorización debe proceder del responsable del tratamiento,

que es quien tiene la plena responsabilidad del mismo. Pero, ¿cómo puede un responsable del tratamiento limitar el tratamiento a lo que está autorizado?

Una respuesta parcial a esta pregunta puede encontrarse en el art. 29 del RGPD: "El encargado del tratamiento y **cualquier persona que actúe bajo la autoridad del responsable del tratamiento** o del encargado del mismo, que tenga acceso a los datos personales, no tratará dichos datos salvo **siguiendo *instrucciones* del responsable del tratamiento**, [..]". También el art. 32(4) del RGPD utiliza una redacción muy similar. El art. 29 del RGPD implica la siguiente concepción:

- La operación de tratamiento es ejecutada por "**una persona física que actúa bajo la autoridad del responsable o del encargado del tratamiento**". Estas personas suelen ser *empleados* del responsable del tratamiento, pero también pueden trabajar para un encargado del tratamiento o trabajar sin estar realmente empleados[80]. En lo sucesivo se denominan ***recursos humanos***. Tenga en cuenta que estas personas controlan a su vez los medios técnicos que apoyan o automatizan parcialmente el tratamiento[81].
- El **medio** con el que un **responsable del tratamiento se asegura de que sólo tiene lugar el tratamiento autorizado** es la emisión de ***instrucciones***.

Para garantizar que sólo se realice el tratamiento autorizado, las instrucciones deben especificar todos los aspectos relevantes de la actividad de tratamiento: quién**, cuándo, qué** y **cómo**. En otras palabras, los recursos humanos tienen que actuar sólo **por instrucción** (quién, cuándo) y **según las instrucciones** (qué, cómo).

Aunque con menos claridad, el RGPD también establece que los **recursos técnicos** son necesarios. Esto queda muy claro en el considerando 39 (frase 12) que habla del "equipo **utilizado para el tratamiento**". Otros términos relacionados con los recursos técnicos que se utilizan en el RGPD son "equipo de tratamiento de datos" en el art. 58(1)(f) y "sistemas de tratamiento" en el Art. 32(1)(b).

Aunque el RGPD utiliza el término *instrucción* sólo en el contexto de los recursos humanos, está claro que **también los recursos técnicos requieren instrucciones** para ejecutar únicamente el tratamiento autorizado. En el ámbito técnico, se utiliza aquí el término instrucciones *de máquina*. Un tipo importante de tales instrucciones es ***el software***.

En resumen, al considerar un **recurso individual** (humano o técnico), el RGPD tiene la siguiente concepción de una operación de tratamiento:

operación de procesamiento individual = **ejecución de** las **instrucciones** del controlador **por un** solo **recurso**

En la mayoría de los casos, el **conjunto de las operaciones de tratamiento** implica un sistema de multitud de recursos humanos y técnicos que interactúan. Esto se expresa de la siguiente manera:

---

80 Véanse también las directrices del Comité Europeo de Protección de Datos (CEPD) sobre los conceptos de responsable y encargado del tratamiento en el RGPD, apartado 88, para analizar el significado de "personas que, bajo la autoridad directa del responsable o del encargado del tratamiento, están autorizadas a tratar datos personales".

81 Hay que tener en cuenta que, incluso en el caso del "procesamiento totalmente automático", siempre es una persona la que controla dicho procesamiento iniciándolo y deteniéndolo. El control por parte de una persona es aún más evidente cuando se trata de "herramientas" informatizadas que son utilizadas por humanos a través de una interfaz hombre-máquina.

operaciones globales de procesamiento **multitud de operaciones** individuales de **procesamiento** ejecutadas **por recursos** humanos y técnicos individuales

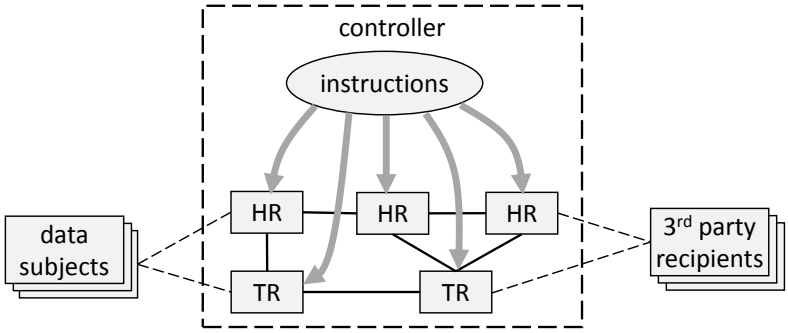

Figura 5: La concepción del RGPD de una operación de tratamiento.

Figura 5 ilustra el concepto de operaciones de tratamiento del RGPD en un contexto más amplio. Ilustra el ámbito de responsabilidad del responsable del tratamiento mediante un recuadro punteado. El responsable del tratamiento determina las operaciones de tratamiento autorizadas emitiendo o seleccionando/aprobando[82] instrucciones tanto a los recursos humanos (RH) que actúan bajo su autoridad (véase el artículo 29 del RGPD) como a los recursos técnicos (RT) bajo su control. Todos los recursos interactúan para formar el sistema global de tratamiento. El contexto de este sistema de tratamiento está definido por *los interesados que* interactúan con los recursos humanos y/o técnicos, y opcionalmente con *terceros destinatarios* (véase el art. 4(9) y (10) del RGPD) a los que los recursos revelan datos personales.

Este modelo de operaciones de tratamiento representa el tratamiento autorizado por el controlador. Se utiliza en la siguiente sección para comprender mejor lo que implica realmente *la determinación de los medios*.

2.3.3.4 Determinación de los medios

En sus directrices sobre los conceptos de responsable y encargado del tratamiento en el RGPD[83], el Comité Europeo de Protección de Datos ofrece un análisis jurídico de lo que significa *determinar los medios* de tratamiento. La discusión aquí está más orientada técnicamente. El Comité distingue entre "medios esenciales" y "medios no esenciales"; estos últimos también pueden ser determinados por los encargados del tratamiento. El presente texto no hace tal distinción y se limita a ofrecer una interpretación técnica de las decisiones que conlleva la determinación de los medios.

La determinación de los medios es una fase que precede a la utilización operativa de un sistema de procesamiento y prepara y establece todo lo necesario para las operaciones de procesamiento propiamente dichas. Esto significa que, guiado por los *propósitos*, un controlador tiene que planificar, diseñar e implementar todo lo necesario para permitir el procesamiento *propiamente dicho*. Esto incluye al menos las siguientes tareas:

82 La selección y aprobación de las instrucciones por parte de un controlador se realiza, por ejemplo, cuando se adquiere un software estándar o cuando un controlador elige el servicio de un determinado procesador.

83 Comité Europeo de Protección de Datos, Directrices 07/2020 sobre los conceptos de responsable y encargado del tratamiento en el RGPD, versión 2.0, adoptadas el 7 de julio de 2021, https://edpb.europa.eu/system/files/2021-07/eppb_guidelines_202007_controllerprocessor_final_en.pdf (última visita: 2/12/2021).

- **Determinar** los **recursos** humanos y técnicos necesarios para el tratamiento;
- **Determinar** las **instrucciones** que **definen el tratamiento autorizado** y que son adecuadas para los recursos;

A continuación, se describe con más detalle lo que esto supone.

La determinación de los recursos humanos implica al menos lo siguiente:

- Planificación que determina qué recursos humanos son necesarios, seleccionando los recursos humanos adecuados y poniéndolos bajo la autoridad del controlador o procesador. Esto suele hacerse mediante una contratación que establece una relación contractual entre el empleado y el responsable del tratamiento.
- Poner a los recursos humanos en condiciones de traducir las instrucciones de manera que constituyan un tratamiento autorizado. Esto puede implicar cosas como
    - la firma de un acuerdo de no divulgación de datos personales,
    - el compromiso del recurso humano con determinadas políticas generales o códigos de conducta, y
    - La formación de los recursos humanos para que adquieran los conocimientos y habilidades necesarios para ejecutar las instrucciones de la forma deseada.

La determinación de los recursos técnicos implica al menos lo siguiente:

- Planificar, seleccionar y adquirir los recursos técnicos necesarios.
- Poner los recursos técnicos en condiciones de ejecutar las operaciones de procesamiento necesarias. Esto puede implicar cosas como
    - instalación física,
    - configuración,
    - integración en la infraestructura utilizada, y
    - instalar el software necesario.

Determinación de las instrucciones para los recursos en general: Después de haber discutido la determinación de los recursos, a continuación, se analiza la determinación de las instrucciones. Observando la Figura 5 está claro que existen los siguientes tipos de instrucciones:

- Instrucciones que determinan el comportamiento de un **único recurso**,
- instrucciones que determinan la **interacción entre** múltiples **recursos**,
- instrucciones que determinan la **interacción** entre los recursos y **los sujetos de los datos**, y
- instrucciones que determinan la divulgación de datos personales a **terceros destinatarios**.

Estos diferentes tipos de instrucciones se analizan con más detalle a continuación, distinguiendo entre recursos humanos y técnicos.

A continuación, se analizan **las instrucciones para los recursos humanos**:

- **Las instrucciones para los recursos humanos individuales** pueden expresarse en dos estilos diferentes:

- Definir los resultados, los productos y los efectos requeridos que debe producir la actividad del recurso humano. Se trata de ***instrucciones declarativas*** que se centran en el aspecto ***del qué*** y confían en la capacidad del recurso para completar el aspecto del *cómo* de las instrucciones.
- Descripciones detalladas de la forma en que debe ejecutarse una actividad. Se trata de ***instrucciones imperativas*** que se centran en el aspecto ***del cómo***, requieren menos inteligencia y autonomía del recurso ejecutor y suelen definir el aspecto del *qué de* forma más implícita.

- **Instrucciones sobre cómo interactúan los recursos humanos entre sí**: Esto incluye el diseño y la especificación de los *procesos empresariales*, los *flujos de trabajo* y *los flujos de datos*. Existen varios lenguajes formales [84]y notaciones[85] gráficas para apoyar estas actividades.
- **Instrucciones sobre cómo interactúan los recursos humanos con los recursos técnicos**: Los recursos técnicos no son autónomos. Más bien son controlados por los humanos (es decir, los recursos humanos). Incluso el recurso técnico más autónomo necesita ser activado. Por lo general, los recursos humanos ejercen un control de mayor alcance sobre el recurso técnico a través de ***interfaces de usuario*** y mediante la *interacción hombre-máquina*. Una forma habitual de modelar estas interacciones son los ***diagramas de casos de uso***. Estos suelen utilizarse también para la *especificación* de los *requisitos funcionales del* software. Las instrucciones sobre cómo interactúan las personas con los recursos técnicos también definen qué recursos humanos están **autorizados a acceder a** qué recursos técnicos y con qué fines. Por tanto, este tipo de instrucciones también determinan la **responsabilidad que** tienen los recursos humanos para operar ciertos recursos técnicos.
- **Las instrucciones sobre el modo en que los recursos humanos interactúan con los interesados** determinan qué interacciones pueden tener los interesados con el responsable del tratamiento. Esto incluye el tratamiento manual de las invocaciones de los derechos de los interesados (véase el capítulo 3 del RGPD) y las interacciones previstas con el delegado de protección de datos (véase el art. 38(4) del RGPD).
- **Las instrucciones sobre el modo en que los recursos humanos interactúan con los terceros** destinatarios determinan qué datos personales se divulgan manualmente a los terceros destinatarios.

La determinación de las instrucciones para los recursos técnicos conlleva lo siguiente:

- **Las instrucciones para los recursos técnicos individuales** abarcan potencialmente los siguientes aspectos:
  - Obtención[86] de ***software*** que suele constituir instrucciones de máquina que se expresan en algún lenguaje de programación formal (imperativo o declarativo). El comportamiento del software puede depender de parámetros que pueden determinarse en un momento posterior; estos parámetros suelen denominarse

84 Estos lenguajes formales incluyen, por ejemplo, el *Lenguaje de Definición de Procesos XML* (XPDL) y el Lenguaje de *Ejecución de Procesos de Negocio* (BPEL).

85 Estas visualizaciones gráficas incluyen, por ejemplo, el *modelo y la notación de procesos empresariales* (BPMN), los *diagramas de actividad*, *los diagramas de flujo* y las *redes de Petri*.

86 La adquisición se utiliza aquí como un término colectivo que abarca tanto el desarrollo a medida como la adquisición de software del mercado. En ambos casos, los controladores son responsables de un adecuado análisis y especificación de los requisitos.

configuración. La decisión de si la configuración es posible y qué parámetros conlleva se incorpora al software. Hay dos tipos de configuración,

- la determinada por el controlador, y
- la controlada por el interesado (por ejemplo, las *preferencias* y los *ajustes* soportados por una interfaz de usuario adecuada).

- ***Configuración*** del software **por parte del controlador**.
- **Especificación de *valores por defecto*** para las configuraciones realizadas por el interesado. Esto es obviamente el tema de la ***Protección de Datos por Defecto*** que se regula en el Art. 25(2) del RGPD (véase la sección 2.3.4 más adelante).

- **Instrucciones sobre cómo interactúan los recursos técnicos entre sí: Los recursos técnicos** pueden interactuar entre sí cuando tienen ***interfaces*** que están conectadas por ***canales de*** comunicación. Las comunicaciones que pueden tener lugar suelen estar determinadas por ***protocolos***. Las comunicaciones pueden representarse, por ejemplo, mediante ***diagramas de interacción*** como los *diagramas de secuencia UML* y *los diagramas de comunicación UML*. Estas comunicaciones suelen implicar el intercambio de datos (personales). Pueden representarse gráficamente en ***diagramas de flujo de datos***. Este tipo de instrucciones también determina qué recursos técnicos están **autorizados** a interactuar con qué otros y con qué fines. Los aspectos determinados por este tipo de instrucciones suelen estar relacionados con el concepto de ***arquitectura técnica (de componentes)***.
- **Las instrucciones sobre cómo interactúan los recursos técnicos con los interesados** suelen utilizarse para la **configuración por parte de los interesados** (véase el artículo 25, apartado 2, del RGPD y su análisis más adelante) y para el apoyo automatizado de los derechos del interesado (véase el capítulo 3 del RGPD). 25(2) del RGPD y su discusión más adelante) y para el apoyo automatizado de los ***derechos de los interesados*** (véase el capítulo 3 del RGPD). Ambos requieren ***interfaces de usuario adecuadas***. Una vez más, se pueden utilizar *diagramas de casos de uso* para representarlas. Una vez más, la ***autenticación*** y el ***control de acceso son necesarios*** para que el recurso técnico determine si el usuario es realmente el interesado legítimo reclamado.
- **Las instrucciones sobre la transferencia automática de datos a terceros destinatarios** determinan qué datos (personales) se revelan, en qué condiciones y cómo. Esto suele requerir interfaces para humanos o máquinas y canales de comunicación adecuados. Los datos pueden ser enviados a los destinatarios o revelados a petición. La autenticación (de personas o máquinas) y el control de acceso también suelen ser relevantes en este caso.

Identificar las medidas técnicas y organizativas adecuadas: Como se ha comentado en la sección 2.3.3.1 anterior, el art. 25(1) obliga a los responsables del tratamiento a aplicar *las medidas técnicas y organizativas apropiadas destinadas a aplicar los principios de protección de datos* también en el momento de determinar *los medios*. Ya se ha explicado que la determinación de los medios consiste en determinar los recursos y las instrucciones. Además, juntos, los recursos y las instrucciones constituyen un sistema de tratamiento capaz de ejecutar las instrucciones autorizadas sobre datos personales reales.

Es evidente que las medidas necesarias deben integrarse en este sistema de tratamiento. Es decir, deben integrarse en sus instrucciones y aplicarse a sus recursos. En otras palabras, estas

medidas no pueden determinarse de forma independiente. Más bien, deben determinarse junto con la determinación de las instrucciones y los recursos. En cada paso de la determinación de una parte o aspecto del sistema de tratamiento, hay que tener en cuenta los principios de la protección de datos para identificar e integrar las medidas adecuadas.

Por esta razón, los aspectos de un sistema de tratamiento que se han distinguido en la discusión anterior identifican directamente las áreas en las que hay que encontrar y aplicar medidas adecuadas. Por lo tanto, esta sección sirve para estructurar el análisis detallado de las medidas que se realiza en la sección siguiente **2.3.3.1**. También sirve para lograr cierta exhaustividad al considerar sistemáticamente todos los aspectos y cada principio.

2.3.3.5 Procesamiento de sí mismo

El tratamiento propiamente dicho se **inicia** con el **visto bueno** del responsable del tratamiento a los recursos para que empiecen a ejecutar las instrucciones emitidas. A partir de este momento, comienza el **tratamiento de los datos personales reales**. Es decir, es ejecutado por los recursos designados que siguen las instrucciones del responsable del tratamiento.

El *tratamiento propiamente dicho* **finaliza** cuando ya no se tratan datos personales. Teniendo en cuenta que según el Art. 4(2) del RGPD, el *almacenamiento* de datos personales constituye un tratamiento, la terminación del *tratamiento en sí* va más allá de decir a los recursos que dejen de ejecutar las instrucciones emitidas. Más bien, requiere también **instrucciones adicionales** para comprobar que los datos personales ya no se almacenan. A esto lo llamamos ***desmantelamiento*** de las operaciones de tratamiento. El desmantelamiento abarca la ***supresión*** y la ***destrucción*** de los datos personales, que siguen constituyendo un *tratamiento de* acuerdo con el artículo 4.2. 4(2).

El art. 25(1) exige que los responsables del tratamiento apliquen también medidas técnicas y organizativas adecuadas durante el propio tratamiento. De forma análoga a la *determinación de los medios*, la estructura encontrada para el tratamiento propiamente dicho se utilizará para orientar el debate sobre las medidas.

2.3.3.6 Redeterminación de los medios durante el tratamiento operativo

Teniendo en cuenta que el resultado de la determinación de los medios son los recursos y las instrucciones, es habitual volver a determinar los medios también durante el procesamiento operativo. Los siguientes ejemplos lo ilustran:

- **Sustitución de los recursos** técnicos que fallan y de los recursos humanos no disponibles. La sustitución de recursos puede ser temporal o permanente.
- **Adición, sustracción o sustitución de recursos** para adaptarse a un **volumen de procesamiento cambiante**. Esto podría incluir, por ejemplo, la adición de recursos humanos a una unidad de trabajo sobrecargada o la sustitución de un recurso técnico por otro más potente.
- **Cambio de instrucciones** para mejorar la **eficiencia y la eficacia**. Esto puede incluir, por ejemplo, la actualización rutinaria del software a la última versión. Otros ejemplos son la mejora evolutiva de las instrucciones o el rediseño de los procesos organizativos.
- Más allá de esto, también es posible una **ampliación de los medios** para apoyar una **ampliación de los fines**. Esto suele ir acompañado de una funcionalidad adicional soportada por el tratamiento.

Dado que esta redeterminación de los medios sigue siendo una determinación de los medios, también aquí el controlador debe aplicar las medidas adecuadas. Por lo tanto, el análisis anterior también se utilizará para estructurar el debate sobre los medios a continuación2.3.3.1.

2.3.3.7 Eficacia de las medidas

A continuación, se analiza el requisito del art. 25(1) del RGPD de que las medidas deben aplicarse "de ***manera efectiva***". Lo hace en el contexto del resto de la redacción del art. 25(1) DEL RGPD.

A diferencia del análisis anterior, el presente no se utilizará para identificar las áreas para las que hay que encontrar medidas. Más bien se utilizará como un aspecto importante que hay que tener en cuenta para cada una de las medidas propuestas.

El art. 25(1) del RGPD obliga a los responsables del tratamiento a aplicar medidas apropiadas "destinadas *a aplicar* ***los principios de protección de datos***" con el fin de "*integrar las* ***garantías*** *necesarias en el tratamiento*". En este contexto, el requisito de eficacia expresa que no es un objetivo en sí mismo la aplicación de medidas. Más bien, las medidas sólo tienen valor en función de su eficacia **para aplicar los principios de protección de datos** e integrar **las garantías**. Por consiguiente, limitarse a aplicar medidas sin tener en cuenta su eficacia sería un ejercicio inútil.

Los contextos en los que debe analizarse la eficacia se establecen en el artículo 25.1 del RGPD en forma de aspectos que los responsables del tratamiento deben tener en cuenta. 25(1) del RGPD en forma de aspectos que los responsables del tratamiento deben tener en cuenta. En concreto, estos aspectos son los siguientes [enumerados en un orden diferente al utilizado en el texto del RGPD]:

- "*los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas que plantea el tratamiento*",
- "*el coste de la aplicación*",
- "*el estado de la técnica*", y
- "*la naturaleza, el alcance, el contexto y los fines del tratamiento*".

Al considerar la eficacia en el **contexto de los riesgos** para las personas físicas afectadas, es evidente que la medida debe ser eficaz para mitigar los riesgos. También implica una cierta proporcionalidad en relación con la magnitud de los riesgos. Al considerar un **conjunto de medidas aplicadas**, su eficacia es **suficiente** si es adecuada para **mitigar el riesgo hasta un nivel aceptable**.

Al considerar la eficacia en el **contexto del coste**, el RGPD parece reconocer que los recursos disponibles para aplicar las medidas son limitados y deben utilizarse de forma eficaz. Esto permite a los responsables del tratamiento utilizar medidas menos costosas y rentables en lugar de otras costosas con un efecto similar. En otras palabras, el criterio es la eficacia, no la asequibilidad o el coste para los responsables del tratamiento como tal. Aunque la consideración del coste deja la posibilidad de que un coste pueda considerarse excesivo, un coste elevado no puede utilizarse como justificación para despreciar la eficacia requerida en diferentes contextos. Si los costes necesarios para asegurar un nivel adecuado de garantías son demasiado elevados para un responsable del tratamiento, éste deberá abstenerse de realizar las actividades de tratamiento.

Si se considera la eficacia en el **contexto del estado de la técnica**, las consecuencias son dobles. Por un lado, evita que los responsables del tratamiento ignoren las nuevas medidas y se abstengan de actualizar el nivel de protección a lo que ofrece el estado de la técnica. Por

otro lado, no se puede obligar a un responsable del tratamiento a aplicar medidas que han sido esbozadas en algún documento de investigación sin haber sido probadas o utilizadas en un entorno operativo. En situaciones en las que los controladores confían en el mercado para proporcionar ciertos tipos de software, puede estar justificado que los controladores limiten las medidas implementadas a las que están realmente disponibles en el mercado, si éstas son suficientes para proporcionar protecciones eficaces. Sin embargo, al igual que en el contexto de los costes, esto no puede eximir de los requisitos de eficacia en otros contextos.

En el contexto de las medidas de seguridad, el estado del arte tiene un significado particular. La ciberseguridad puede verse como una carrera armamentística entre *hackers* y defensores. En un panorama de amenazas en constante evolución, cada vez que los defensores piensan en medios más eficaces para frustrar los ataques, los *hackers* encuentran medios de ataque más sofisticados. Esto hace evidente que el concepto de "defensa eficaz" está en constante movimiento. En este contexto, la información actual sobre las amenazas y las defensas disponibles es importante a la hora de evaluar la eficacia de las medidas aplicadas. Asimismo, la no aplicación de nuevas medidas, por ejemplo, en forma de actualizaciones o parches críticos para la seguridad, no puede ser justificada por los responsables del tratamiento (salvo en el raro caso de que las nuevas medidas sean irrelevantes para las actividades de tratamiento y los riesgos relacionados).

Obsérvese que el Comité Europeo de Protección de Datos (CEPD) señala en sus directrices sobre la protección de datos por diseño y por defecto que el estado de la técnica no se define únicamente por las medidas técnicas, sino que también incluye medidas organizativas como marcos, normas, certificaciones y códigos de conducta[87].

Al considerar la eficacia en relación con la **naturaleza, el alcance, el contexto y los fines del procesamiento, se** reconoce que las medidas tienen que ajustarse al procesamiento en cuestión. Una medida que es eficaz para un sistema de información tradicional que apoya a los seres humanos que toman decisiones puede no ser eficaz cuando se aplica a una aplicación de aprendizaje automático que toma decisiones automáticas; una medida que funciona bien para el procesamiento de bajo volumen en un entorno pequeño puede no ampliarse a un procesamiento de alto volumen; y una medida que funciona eficazmente cuando se utilizan procesadores de confianza (que a su vez están sujetos al RGPD) puede no ser eficaz y suficiente cuando se utilizan procesadores menos confiables (como los ubicados en 3rd países y no están obligados por el RGPD).

El art. 5(2) exige que los responsables del tratamiento puedan demostrar el cumplimiento del RGPD. Un aspecto importante de esto es poder demostrar que las medidas aplicadas son realmente eficaces. Debe ser parte integrante del proceso de toma de decisiones sobre las medidas a aplicar. Las dimensiones de la eficacia se indican en el artículo 25, apartado 1, y se han analizado. 25(1) y se han discutido anteriormente.

2.3.4 Análisis de la protección de datos por defecto en el art. 25(2) del RGPD

A continuación, se analizarán los requisitos del Art. 25(2) del RGPD. Se utiliza la definición de los incumplimientos proporcionada en la sección de *determinación de las instrucciones para los recursos técnicos* en este documento"(1.3.3).

Como se desprende de la definición anterior, los valores por defecto se refieren a los ajustes (a veces denominados *preferencias* o *perfil de usuario*) que están bajo el control del

[87] Véase el apartado 22 de las directrices del Comité Europeo de Protección de Datos (CEPD) sobre la protección de datos por diseño y por defecto (*Data Protection by Design and Default* o *DPbDD*).

interesado. Los responsables del tratamiento deciden sobre los ajustes **por defecto, es** decir, los **ajustes** que están activos **en ausencia de cualquier intervención por parte del interesado**.

Estos ajustes influyen en el procesamiento que tiene lugar, incluyendo los siguientes aspectos:

- los datos personales que se están tratando,
- el grado de procesamiento que se realiza,
- el periodo de almacenamiento de los datos, y
- las personas físicas a las que se les hace accesible los datos personales.

El siguiente ejemplo de configuración lo ilustrará:

- Los interesados pueden proporcionar opcionalmente una **dirección de correo electrónico** para **ser informados del estado de tramitación de un pedido**. Evidentemente, esto afecta a la cantidad de datos personales que trata el responsable del tratamiento. También afecta al alcance del tratamiento.
- Para procesar un pedido, los interesados siempre tienen que proporcionar una **dirección de envío y la información de pago**. Opcionalmente, pueden hacer clic en una casilla para **recordar** esta información y **evitar tener que escribirla repetidamente** para futuros pedidos. Aunque la cantidad de datos procesados por el responsable del tratamiento es siempre la misma, la opción controlada por el usuario afecta obviamente al periodo de almacenamiento de esos datos.
- Un proveedor de redes sociales puede presentar a sus usuarios una configuración **de privacidad** que controle la **visibilidad de sus publicaciones**, desde *sólo los amigos cercanos* hasta *todo el mundo.* Evidentemente, esta configuración de privacidad controla las personas físicas que tienen acceso a las publicaciones, que representan datos personales.

El RGPD incluye lo siguiente:

Art. 25(2):

El responsable del tratamiento aplicará las medidas técnicas y organizativas adecuadas para garantizar que, por defecto, sólo se traten los datos personales necesarios para cada finalidad específica del tratamiento. Esta obligación se aplica a la cantidad de datos personales recogidos, al alcance de su tratamiento, al período de su almacenamiento y a su accesibilidad. En particular, dichas medidas garantizarán que, por defecto, los datos personales no sean accesibles, sin la intervención del individuo, a un número indefinido de personas físicas.

El art. 25(2) ordena así que, **por defecto**, el tratamiento se **limitará** a lo **necesario para los fines**. Además, aclara que esto debe entenderse con respecto a la **cantidad de datos**, el **alcance del tratamiento** y el **periodo de almacenamiento de los datos**. La tercera frase establece que esto también es aplicable[88] al número de personas a las que se hace accesible los datos. Por lo tanto, esto parece referirse al número de destinatarios (tal como se define en el Art. 4(9) del RGPD).

88 "En particular" indica que el resto de la frase es una aplicación de la expresión de la frase anterior.

La redacción del art. 25(2) implica que debe haber algunos tipos de fines adicionales: por defecto, el tratamiento debe limitarse a un determinado conjunto de fines; pero tras la intervención del interesado, evidentemente el tratamiento va más allá de esta limitación. Esto implica que el tratamiento persigue fines adicionales.

Los ejemplos anteriores ayudan a entenderlo mejor. En el primer ejemplo, la finalidad adicional es **mantener informado al interesado sobre el estado de tramitación de los** pedidos. En el segundo ejemplo, la finalidad adicional es mejorar **la comodidad del usuario** para aquellos sujetos de datos que esperan volver a realizar pedidos en el futuro. En el tercer ejemplo, no se persigue ninguna finalidad adicional. Más bien, la finalidad de restringir la visibilidad de las publicaciones en las redes sociales al **ámbito previsto por el usuario**, está siempre presente. Obsérvese que la tercera frase del art. 25(2) que se ajusta a este ejemplo también se abstiene de hacer referencia a los fines.

Estos ejemplos ilustran que los **fines adicionales** y los fines que subyacen a la situación contemplada en la tercera frase son siempre **fines que benefician a los interesados**.

Sobre la base de este análisis, el art. 25(2) parece establecer que **por defecto**:

- **Los fines adicionales** que puedan beneficiar a los interesados serán **inhabilitados**, al menos mientras requieran la recogida de datos adicionales, aumenten el alcance del tratamiento, provoquen una ampliación del período de almacenamiento o aumenten el número de destinatarios;
- cuando el tratamiento persiga siempre una finalidad en interés del interesado (es decir, que no se pueda desactivar), su **impacto en la protección de datos debe reducirse al mínimo con respecto a los** datos recogidos, el alcance del tratamiento, el período de almacenamiento y el número de destinatarios.

El art. 25(2) puede considerarse una especie de **protección contra las "puertas traseras"** en las que los responsables del tratamiento recogen datos adicionales, los almacenan durante períodos más largos, aumentan el alcance del tratamiento o los destinatarios, con la justificación de que era el deseo del interesado. Evidentemente, los sujetos de los datos que no han intervenido de ninguna manera, pueden ni siquiera ser conscientes de "sus deseos", pueden no haber leído la expresión de sus deseos en detalle, o al menos están influenciados por los valores por defecto para expresar más probablemente los "deseos" favorecidos por el responsable del tratamiento.

Esta salvaguardia, que requiere explícitamente la intervención del interesado, impone el uso de diálogos de inclusión y prohíbe los diálogos de exclusión. Es el mismo concepto que se denomina "acción de afirmación clara" en el contexto del consentimiento (véase el art. 4(11) del RGPD). Es directamente comparable a la afirmación de que, sin una acción afirmativa clara, es decir, "***sin la intervención del individuo",*** es ilegítimo el tratamiento adicional en términos de cantidad y período de almacenamiento de datos, alcance del tratamiento o número de destinatarios. Es importante señalar que este requisito de soluciones de inclusión voluntaria es independiente de si se elige el *consentimiento* como base jurídica o no.

Sobre la base del análisis anterior, las medidas mencionadas en el art. 25(2) podrían ser las siguientes:

- Medidas que garantizan que la configuración por defecto minimiza el impacto de la protección de datos del tratamiento.
- Medidas que garantizan que los interesados sean informados de las consecuencias de los ajustes que están bajo su control.

- Medidas que aseguren que las decisiones expresadas por los ajustes son específicas. Por ejemplo, los propósitos adicionales no pueden habilitarse todos con una sola casilla de verificación, sino que debe ser posible habilitarlos individualmente.
- Medidas que verifiquen la ausencia de cualquier tipo de empuje en el diálogo en el que los usuarios eligen sus configuraciones, con el fin de garantizar que el sujeto de los datos pueda elegir libremente sus preferencias.

2.3.5 Aplicación de los principios de protección de datos en las distintas fases del tratamiento

El objetivo de la protección de datos desde el diseño es integrar (o aplicar) en todas las fases de una actividad de tratamiento medidas técnicas y organizativas adecuadas que apliquen los principios de protección de datos.

Las directrices del Comité Europeo de Protección de Datos (CEPD), sobre la protección de datos por diseño y por defecto *(Data Protection by Design and Default o DPbDD)* contienen una sección importante sobre la "aplicación de los principios de protección de datos en el tratamiento de datos personales utilizando la protección de datos desde el diseño y por defecto". Está estructurada por los principios de protección de datos que deben aplicarse. Las directrices del Comité Europeo de Protección de Datos no abordan la cuestión de cómo aplicar la protección de datos por diseño y por defecto en las distintas fases.

Esta sección sobre cómo aplicar los principios de protección de datos no se centra en una descripción de los principios en sí, como hacen las directrices de la Comité Europeo de Protección de Datos (independientemente de las fases); ya se proporcionó una descripción detallada de las directrices en el capítulo correspondiente de las directrices de PANELFIT (véase la Parte II de estas directrices, sección "Principios"). Más bien, esta sección trata de los procesos que pueden utilizarse para aplicar estos principios en cada una de las tres fases que se identificaron en el análisis del art. 25(1) anterior.

Así pues, lo que es común a las tres fases es que utilizan los ***principios* de la *protección de* datos** *en* cada paso de trabajo (o decisión) para

- **identificar los riesgos** que conducen a la violación o a la aplicación inadecuada de un principio, y
- **identificar** las **medidas** técnicas y organizativas adecuadas que mitiguen estos riesgos.

Las medidas reales a aplicar dependen en gran medida de la naturaleza, el alcance, el contexto y los fines del tratamiento. Por lo tanto, no es posible ofrecer una lista completa de medidas apropiadas para cada tupla de fase (o tarea dentro de una fase) y principio. Por ello, esta sección describe el proceso de identificación de las medidas adecuadas. En la sección correspondiente de las Directrices se ofrece un análisis detallado (con ejemplos) de las medidas para aplicar los distintos principios.

A continuación, se analizan con más detalle las fases de *determinación de los fines*, *determinación de los medios* y el *propio tratamiento*.

2.3.5.1 Determinación de los objetivos

Una actividad de tratamiento se concibe determinando sus fines. Esto establece el objetivo de lo que la actividad de procesamiento debe lograr. Esta especificación del "qué" debe hacerse

sigue siendo relativamente abstracta y carece de detalles sobre el "cómo" se alcanza este objetivo. El "cómo" está sujeto a la determinación de los medios.

Los propósitos suelen ser determinados por la alta dirección que representa y es responsable de una organización (o unidad organizativa). Los propósitos suelen expresarse en el mismo lenguaje en el que se expresa la misión o el mandato de la organización. Es decir, proceden del "dominio de la aplicación" y carecen de contenido técnico. Una especificación de propósito no llega a determinar decisiones técnicas como qué recursos (es decir, medios) se necesitan para alcanzar los objetivos, qué datos hay que recoger, etc. Más bien, una especificación de propósito puede aplicarse de muchas maneras diferentes. El objetivo de la determinación de los medios es entonces encontrar la mejor implementación desde el punto de vista de la protección de datos.

Según el art. 5(1)(a) del RGPD, los fines deben ser "específicos [y] explícitos". Esto significa que deben plasmarse de forma precisa y por escrito.

La determinación de los fines del tratamiento suele ser un proceso iterativo. Empezando por la finalidad o finalidades principales, la especificación se va completando y perfeccionando continuamente hasta llegar a una versión final. Cada versión debe evaluarse teniendo en cuenta los principios de protección de datos, las expectativas razonables de los interesados y el riesgo general que puede suponer el tratamiento. Sobre la base de esta evaluación, se introducen mejoras en la especificación de la finalidad que mejoran la observancia de los principios, están más equilibradas con las expectativas de los interesados y mantienen el equilibrio entre la necesidad/beneficio del tratamiento y el riesgo que supone para los interesados. Las iteraciones pueden verse como un proceso para encontrar el mínimo impacto en los derechos y libertades de los sujetos de los datos sin dejar de alcanzar los objetivos esenciales de la organización. Normalmente, en cada integración, la especificación de la finalidad se vuelve más centrada, más estrecha y específica e impone un menor impacto en los sujetos de los datos.

Este proceso se visualiza en Figura 6.

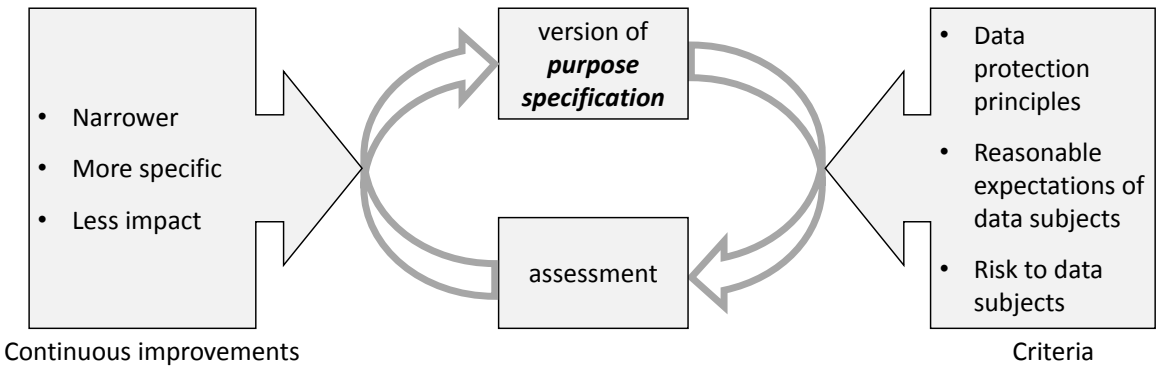

Figura 6: El proceso de especificación de la finalidad

La protección de datos desde el punto de vista del diseño aplica los principios de la protección de datos a cada paso de la determinación. Aunque algunos de los principios de protección de datos son más aplicables a los medios de tratamiento, la *legitimidad*, la *legalidad* y la *equidad* son directamente aplicables a los fines. Indirectamente, también es aplicable la minimización de los datos en el sentido de que debe minimizarse el impacto del tratamiento sobre los interesados. Esto suele traducirse en una minimización de los datos que se recogen sobre los interesados. Obsérvese también que la limitación de la finalidad durante la determinación de

los medios sólo tiene sentido si los fines se especifican de forma estricta; sólo entonces puede determinarse con precisión si los datos o los pasos del tratamiento son realmente necesarios para los fines. Los principios fundamentales se analizan con más detalle a continuación.

Legalidad (véase "Legalidad, equidad y transparencia" en la sección "Principios" de la Parte II de estas Directrices):

De acuerdo con el Art. 6 del RGPD, el tratamiento es lícito si se aplica una de las **bases jurídicas** descritas en su apartado 1. El art. 9 del RGPD añade requisitos adicionales para las categorías especiales de datos. Para cumplir con el principio de *legalidad*, el controlador debe elegir una base legal del Art. 6 y posiblemente 9 del RGPD para cada uno de los fines que se persiguen con la actividad de tratamiento.

Obsérvese que es habitual que una actividad de tratamiento persiga una multitud de fines que utilizan diferentes bases jurídicas. Bruegger *et ál*[89]. describieron una ilustración de esto utilizando el ejemplo de las compras en línea.

Legitimidad (véase "Legalidad, equidad y transparencia" en la sección "Principios" de la Parte II de estas Directrices):

Mientras que la legalidad se refiere a los artículos 6 y 9 del RGPD. 6 y 9 del RGPD, la legitimidad exige cumplir la ley en el sentido más amplio. Por tanto, no se limita al RGPD, sino que se extiende a cualquier otra ley aplicable. Podría decirse que las leyes no solo deben seguirse al pie de la letra, sino también en espíritu. En muchas situaciones, la legitimidad también puede interpretarse de manera que incluya el derecho no vinculante, como los requisitos éticos y las normas profesionales de uso común. Incluso puede extenderse a la protección de los valores de la sociedad en general.

La evaluación de la legitimidad de los fines depende en gran medida de la naturaleza, el alcance y el contexto del tratamiento. En algunos casos, el cumplimiento de la legitimidad puede requerir pasos formales. Esto es típico, por ejemplo, en las organizaciones de investigación en las que una actividad de tratamiento debe ser aprobada preventivamente por un comité de ética de la investigación.

Imparcialidad (véase "Legalidad, imparcialidad y transparencia" en la sección "Principios" de la Parte II de estas Directrices):

Un elemento clave de la equidad es tener en cuenta las expectativas y situaciones razonables de los interesados. Los intereses del responsable del tratamiento, expresados en la especificación de la finalidad, se equilibran con los de los interesados. La repercusión en los derechos y libertades de los interesados debe justificarse con un nivel acorde de necesidad y beneficios potenciales para el responsable del tratamiento.

La evaluación de la equidad de los fines suele requerir la evaluación de las expectativas de los interesados. Hay varias formas de hacerlo, desde "ponerse en el lugar de los interesados" hasta implicar a las organizaciones de consumidores o realizar encuestas.

Para evaluar las expectativas de los interesados, a menudo resulta útil distinguir diferentes personas que representan distintos tipos y situaciones de interesados. También deben incluirse sujetos de datos especialmente vulnerables (como menores o pacientes), o grupos de sujetos

89 Bud P. Bruegger, Eva Schlehahn y Harald Zwingelberg, *Data Protection Aspects of Online Shopping - A Use Case, W3C Data Privacy Vocabularies and Controls Community Group*, 12 de diciembre de 2019, https://www.w3.org/community/dpvcg/2019/12/12/data-protection-aspects-of-online-shopping-a-use-case/ (Última visita: el 15/7/2021).

de datos que pueden verse afectados por el tratamiento de forma mucho más significativa que la media.

La ponderación debe considerar los riesgos que la actividad de tratamiento representa para los derechos y libertades de los interesados. Los 9 criterios del Grupo de Trabajo de Protección de Datos del Artículo 29 proporcionan una rápida evaluación general del riesgo para [90]determinar si una actividad de tratamiento conlleva un alto riesgo (y, por tanto, requiere una evaluación de impacto sobre la protección de datos). Esto debería complementarse con un análisis de cómo las categorías especiales de interesados y los interesados vulnerables se ven afectados por la actividad de tratamiento prevista.

Tenga en cuenta que se requiere formalmente una prueba de equilibrio cuando la base jurídica del *interés legítimo* (véase el art. 6(1)(f) del RGPD) para un fin determinado. El Grupo de Trabajo sobre Protección de Datos del Artículo 29 proporcionó orientaciones sobre cómo realizar una prueba de sopesamiento en este contexto [91](véase "Interés legítimo y prueba de sopesamiento", sección de la Parte II "Principales herramientas y acciones"). En un contexto más general, el SEPD ha proporcionado directrices sobre la proporcionalidad[92].

2.3.5.2 Determinación de los medios

La siguiente subsección describe cómo identificar las medidas técnicas y organizativas adecuadas a la hora de determinar los medios.

Mientras que la determinación de los fines del tratamiento especifica el "qué" debe lograrse con el tratamiento, la determinación de los medios especifica el "cómo" se logra este objetivo. En cada paso de la determinación de este "cómo", deben tenerse en cuenta los principios y requisitos de la protección de datos.

La determinación de los medios puede considerarse el resultado de un *plan de ejecución* de la actividad de tratamiento. Este plan implica recursos, instrucciones y medidas técnicas y organizativas. Estas últimas están diseñadas para aplicar los principios de protección de datos. Para un análisis detallado de las medidas que aplican los distintos principios, véase la sección de las Directrices sobre los principios (véase la sección "Principios" dentro de la Parte II de estas Directrices).

2.3.5.2.1 *Gestionar el proceso de determinación de los medios*

La determinación de los medios suele ser un proceso importante en el que suelen intervenir multitud de personas, ámbitos de conocimiento, unidades organizativas o departamentos, y en el que incluso pueden participar consultores y expertos externos.

Por lo tanto, la **principal medida organizativa** (meta) consiste en **establecer el proceso de determinación de los medios de manera** que cumpla con la protección de datos por diseño. Esta medida se denomina "metamedida", ya que está destinada a identificar las medidas que

90 Véanse las páginas 9 - 11 del Grupo de Trabajo de Protección de Datos del artículo 29, WP 248rev.01, Directrices sobre la evaluación de impacto de la protección de datos (EIPD) y la determinación de si el tratamiento es "probable que dé lugar a un alto riesgo" a los efectos del Reglamento 2016/679, Adoptado el 4 de abril de 2017. Como último revisado y adoptado el 4 de octubre2017, https://ec.europa.eu/newsroom/article29/items/611236 (última visita 15/7/2021).

91 en Artículo 29 Grupo de Trabajo de Protección de Datos, WP217, Dictamen 06/2014 sobre la noción de intereses legítimos del responsable del tratamiento en virtud del artículo 7 de la Directiva 95/46/CE, Adoptado el 9 de abril de 2014, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf (última visita 15/7/2021).

92 Supervisor Europeo de Protección de Datos, Directrices del SEPD sobre la evaluación de la proporcionalidad de las medidas que limitan los derechos fundamentales a la intimidad y a la protección de los datos personales, 19 de diciembre de 2019, https://edps.europa.eu/data-protection/our-work/publications/guidelines/assessing-proportionality-measures-limit_en (última visita el 15/7/2021).

realmente aplican los principios de protección de datos. La metamedida debe asignar responsabilidades claras a la alta dirección:

- La alta dirección que representa legalmente al responsable del tratamiento tiene que controlar este proceso y ordenar que la protección de datos se tenga debidamente en cuenta en cada paso y decisión.
- La alta dirección debe ser capaz de diseñar si los medios determinados (es decir, el resultado de este proceso) cumplen realmente con los requisitos de protección de datos.
- Al final de este proceso, es responsabilidad de la alta dirección dar el visto bueno a los medios determinados y dar el visto bueno a las operaciones de tratamiento propiamente dichas (el tratamiento propiamente dicho).

Existen diferentes **medidas** (meta) **organizativas posibles para** conseguirlo. A continuación se enumeran algunos ejemplos:

- Cada paso o decisión tomada como parte de la determinación de los medios debe describir los requisitos de protección de datos pertinentes y cómo se han aplicado o satisfecho de otra manera.
- Si se opta[93] [94] por un enfoque por etapas, cualquier transición de las mismas debe estar sujeta a la aprobación de los aspectos de protección de datos.
- Debe hacerse una designación clara de las personas responsables de determinar si se han cumplido los requisitos de protección de datos en las distintas etapas.
- Cuando se disponga de él, el responsable[95] de la protección de datos debe participar en el proceso.
- (La documentación (continua) de la consideración e incorporación de la protección de datos debe ser una parte integral del proceso. Esto sirve tanto para satisfacer el principio de *responsabilidad* (véase el art. 5(2) del RGPD) y como base para la determinación por parte de la alta dirección de su decisión de aprobar formalmente el resultado que se utilizará operativamente (es decir, un visto bueno para el *tratamiento en sí*).

El proceso de determinación de los medios necesita inevitablemente **evaluar la eficacia** de las distintas medidas (véase el debate sobre la eficacia en la sección 2.3.3.7 anterior). Para ello suele ser necesario realizar

- evaluaciones de riesgo y
- estudios del estado de la técnica o del mercado.

Tenga en cuenta que la herramienta formal prevista en el RGPD para evaluar la eficacia de las medidas de protección de datos es la *Evaluación de Impacto de la Protección de Datos (EIPD*, véase el artículo 35 del RGPD) (véase "EIPD", Parte II, sección "Principales herramientas y acciones"). Tanto la evaluación de riesgos como la descripción de las medidas están contenidas en sus partes obligatorias. El RGPD sólo exige formalmente una Evaluación

93 Véase, por ejemplo, https://en.wikipedia.org/wiki/Phase-gate_process (última visita: 13/7/2021).

94 Tenga en cuenta que las etapas no se limitan a la gestión "en cascada", sino que también existen en los métodos ágiles, como el Proceso Unificado, Ágil véase http://www.ambysoft.com/unifiedprocess/aup11/html/phases.html (última visita el 13/7/2021).

95 Tenga en cuenta que el responsable de la protección de datos no es el responsable directo del cumplimiento, pero es el experto interno que probablemente esté más familiarizado con los requisitos del RGPD (véase también el art. 39(1)(a) a (c) del RGPD).

de Impacto relativa a la Protección de Datos (EIPD) en presencia de un riesgo elevado, pero puede utilizarse de manera informal dentro del proceso interno. Una EIPD es también una herramienta primordial para documentar el cumplimiento de la protección de datos por diseño.

Al menos las grandes organizaciones con varias actividades de procesamiento distintas pueden beneficiarse de la utilización de un **enfoque** más **sistemático** para determinar los medios. Esto puede incluir lo siguiente:

- El uso de ***políticas de protección de datos*** que son aplicables a múltiples actividades de tratamiento y que, por tanto, pueden aportar una economía de escala (véase el art. 24(2) del RGPD).
- La identificación y aplicación de códigos de conducta aplicables en todo el sector puede ahorrar esfuerzos y mejorar la calidad de la aplicación (véase el art. 24(3) del RGPD).

El **resultado final** de un proceso exitoso de determinación de los medios es una aprobación clara y documentada de los mismos y un visto **bueno** por parte de la alta dirección que representa al responsable del tratamiento. El visto bueno es necesario para que el responsable del tratamiento asuma la plena responsabilidad del mismo (véase el artículo 29 del RGPD). Como base adicional para la decisión de autorización, los responsables del tratamiento pueden solicitar **una certificación formal** con arreglo al artículo 42 del RGPD. 42 del RGPD (véase el art. 24(3) del RGPD). La certificación representa un certificado formal de cumplimiento del RGPD. Un visto bueno documentado es un requisito previo para el inicio de la fase operativa del tratamiento (el *tratamiento propiamente dicho*).

2.3.5.2.2 *Evaluación de la eficacia de las medidas relativas a los principios de protección de datos*

El proceso anterior debe adoptar un enfoque sistemático para aplicar todos los principios de protección de datos de forma sistemática a todas las decisiones sobre medios. En particular, cada principio debe aplicarse con medidas técnicas y organizativas. Hay que demostrar que estas medidas son eficaces en lo que respecta a

- "los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas que plantea el tratamiento",
- "el coste de la aplicación",
- "el estado de la técnica", y
- "la naturaleza, el alcance, el contexto y los fines del tratamiento"

(véase la sección 2.3.3.7 anterior).

Cuando se evalúa el riesgo (véase el primer punto), un riesgo básico es que el principio se viole o se garantice insuficientemente. Este puede ser el caso de todos los interesados o de grupos especiales o minorías. Deben tenerse en cuenta los sujetos de datos vulnerables que posiblemente se hayan identificado durante la determinación de los fines (véase la sección 2.3.5.1).

Para evaluar el tercer aspecto de la eficacia, puede ser necesario realizar encuestas sobre el estado de la técnica.

Una forma de evaluar la eficacia de las medidas es utilizar un enfoque iterativo muy similar al utilizado para determinar los propósitos (véase Figura 6). En lugar de una versión de la *especificación de los propósitos*, se evalúa un *plan de aplicación* concreto. Este plan conlleva

tanto recursos como instrucciones y medidas técnicas y organizativas ya previstas (véase la sección "Principios" de la Parte II de estas Directrices). En cada iteración, se evalúa la eficacia de las medidas y se mejora el plan en función de las deficiencias detectadas. El proceso iterativo termina entonces cuando se ha encontrado un plan de aplicación con medidas eficaces.

Para que este proceso sea sistemático, cada tarea que dé lugar a una decisión sobre los medios tiene que ser evaluada con respecto a todos los principios. En la sección 2.3.3.4 anterior ha proporcionado una visión general de las posibles tareas. Sin embargo, el desglose preciso de la determinación global en tareas depende de la naturaleza, el alcance, el contexto y los fines de la actividad de tratamiento. Por lo tanto, es necesario adaptar el desglose en tareas a la situación concreta.

2.3.5.3 Procesamiento de sí mismo

A continuación, se examina la aplicación de los principios de protección de datos durante la fase operativa, es decir, el tratamiento propiamente dicho.

La transparencia y la **equidad** son probablemente los principios más relevantes en esta fase (véase "Legalidad, equidad y transparencia" en la Parte II, sección "Principios"). Exigen, entre otras, las siguientes medidas técnicas y organizativas:

- El tratamiento eficaz de las invocaciones de los derechos de los interesados.
- La gestión de las violaciones de datos personales.

Al final de una actividad de tratamiento, (el aspecto temporal de) la **minimización de los datos** (véase la "Minimización de los datos" en la Parte II, sección "Principios fundamentales" de estas Directrices): requiere que se borren los datos personales que ya no son necesarios para los fines. Existen diversas medidas para garantizar que los datos se borren de forma irreversible y que se tengan en cuenta todos los dispositivos técnicos de almacenamiento antes de su desmantelamiento. Estas medidas también apoyan el principio de **limitación de la finalidad** (véase "Limitación de la finalidad" en la Parte II de estas Directrices, sección "Principios"): ya que si no se borran los datos se abre la posibilidad de que se utilicen para otros fines. La eficacia de las medidas utilizadas para el desmantelamiento debe verificarse y documentarse como se ha descrito en la sección 2.3.5.2.2 anterior.

El art. 5(1)(b) del RGPD prevé la posibilidad de un **tratamiento posterior para fines compatibles**. El principio de **limitación de la finalidad** requiere una evaluación cuidadosa (de acuerdo con el Art. 6(4) RGPD) si estos fines son realmente compatibles. Este tratamiento posterior también requiere la aplicación de medidas adicionales, como la **minimización de los datos**, la seudonimización o la anonimización (es decir, la limitación **del almacenamiento**), con el fin de garantizar las **garantías** exigidas en el artículo 89, apartado 1, del RGPD. 89(1) del RGPD.

Aunque la **eficacia de las medidas** se ha verificado inicialmente durante la determinación de los medios, la segunda frase del art. 24(1) del RGPD exige que se **revise periódicamente** y que se actualicen las medidas cuando sea necesario. Tales revisiones y actualizaciones son medidas en sí mismas.

A continuación, se enumeran ejemplos de dónde se realizan estas revisiones:

- Los derechos de acceso del personal que garantizan la **confidencialidad** y la **limitación de la finalidad** pueden tener que actualizarse para reflejar los cambios de personal y el fin de las asignaciones temporales y las sustituciones.

- Los programas informáticos que garantizaban la **confidencialidad** pueden dejar de hacerlo a menos que se instalen actualizaciones de seguridad críticas.
- **La confidencialidad que se consideraba** suficiente puede dejar de serlo si el **panorama de las amenazas** evoluciona y son posibles **nuevos tipos de ataques**. Normalmente, esto requiere la aplicación de medidas adicionales o más sofisticadas.
- Es posible que haya que presumir el **anonimato de** los datos o impedir su identificación directa (en el marco de la seudonimización), pero los **nuevos métodos de reidentificación** ponen en entredicho estas presunciones. Para seguir apoyando la **limitación del almacenamiento**, es necesario reducir aún más el potencial de identificación de los datos en cuestión o rediseñar el tratamiento.

Una situación similar se presenta durante la **sustitución rutinaria de recursos** (humanos y técnicos). Cuando, por ejemplo, se comprueba que una persona tiene la formación y las habilidades suficientes para ejecutar un conjunto de instrucciones, es necesario realizar el mismo tipo de evaluación para los sucesores de esta persona. Del mismo modo, los nuevos recursos técnicos deben presentar las mismas propiedades que garantizaban la eficacia del componente original.

Las instrucciones suelen evolucionar a lo largo de la vida de una actividad de procesamiento. Las instrucciones para los recursos humanos y los flujos de trabajo pueden, por ejemplo, rediseñarse o hacerse más eficientes en función de la experiencia. Las instrucciones para los recursos técnicos suelen cambiar con cada versión del software y a menudo se instalan automáticamente (por ejemplo, mediante un servicio de actualización). Con cada nueva versión de las instrucciones, hay que verificar lo siguiente:

- Que la nueva versión siga implicando las medidas necesarias para garantizar la aplicación efectiva de los principios
- que no se produzca un "desvío de funciones" que amplíe el tratamiento más allá de lo necesario para los fines.

Cuando el cambio de recursos o instrucciones es más sustancial, puede ser necesaria una nueva iteración completa del proceso iterativo de determinación de los medios (véase la sección 2.3.5.2.2) puede ser necesaria.

2.4 Protección de datos e investigación científica

Pilar Nicolás Jiménez[96] *(UPV/EHU), Mikel Recuero Linares (UPV/EHU)*

Esta parte de las Directrices fue revisada por Rossana Ducato

Esta parte de las Directrices ha sido revisada y validada por Marko Sijan, Asesor Superior Especialista, (HR DPA)

96 Esta sección incorpora algunas referencias extraídas del capítulo de un libro del autor, publicado originalmente en español: *Comentarios al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales* (Antonio Troncoso Reigada, Dir.), Thomson Reuters Aranzadi, 2020.

2.4.1 Puntos clave

- El RGPD es consciente de la importancia primordial que pueden tener las operaciones de tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos.
- Por lo tanto, el Reglamento prevé un régimen especial y favorable en un intento de garantizar que las normas de protección de datos no constituyan un obstáculo importante para las operaciones de tratamiento con los fines mencionados.
- En este sentido, se establece expresamente como condición para el tratamiento de categorías especiales de datos personales, su necesidad para fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos.
- El texto también establece un régimen flexible para el almacenamiento de datos a largo plazo y una presunción de compatibilidad para fines secundarios o posteriores.
- Además, se prevén limitaciones, excepciones o derogaciones, *entre otros,* a los derechos de información, acceso, rectificación, restricción del tratamiento, oposición y, en lo que respecta a los fines de archivo en interés público, al derecho de notificación y portabilidad.
- Con el fin de lograr un equilibrio adecuado con los derechos e intereses de los interesados, el Reglamento exige la adopción de garantías adecuadas de conformidad con el artículo 89 y, en determinadas situaciones, también el desarrollo de la legislación de la Unión o de los Estados miembros.

2.4.2 Introducción

Como ha destacado el Supervisor Europeo de Protección de Datos (SEPD), "la Comisión Europea ha definido como objetivos de las políticas de investigación e innovación de la UE "abrir el proceso de innovación a personas con experiencia en ámbitos distintos del académico y el científico", "difundir los conocimientos tan pronto como estén disponibles utilizando la tecnología digital y colaborativa" y "promover la cooperación internacional en la comunidad investigadora".[97] Estos objetivos no entran en conflicto con la protección de datos. De hecho, las normas de protección de datos no deben ser un obstáculo para la libertad de la ciencia de acuerdo con el artículo 13 de la Carta de los Derechos Fundamentales de la UE. Por el contrario, estos derechos y libertades deben evaluarse y equilibrarse cuidadosamente, dando lugar a un resultado que respete la esencia de ambos[98].

De hecho, la intención de nuestra actual legislación sobre protección de datos es armonizar el tratamiento de datos con los fines de la investigación científica.[99] Esta intención está claramente vinculada al artículo 179, apartado 1, del Tratado de Funcionamiento de la Unión Europea (TFUE) para lograr un Espacio Europeo de Investigación. En consonancia con ello, el Reglamento General de Protección de Datos (RGPD) ha introducido un nuevo marco destinado a permitir el tratamiento de datos con fines de archivo en interés público, fines de

[97] SEPD, Dictamen preliminar sobre la protección de datos y la investigación científica, 2020, p. 10. En: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_en.pdf Consultado: 15 de enero de 2020.

[98] Comité Europeo de Protección de Datos (CEPD), Directrices 03/2020 sobre el tratamiento de datos relativos a la salud con fines de investigación científica en el contexto del brote de COVID-19. Adoptadas el 21 de abril de 2020, p. 5. En: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_en.pdf Consultado el 23 de abril de 2020.

[99] Considerando 159 RGPD.

investigación histórica y científica o fines estadísticos que va más allá de lo previsto en la Directiva 95/46/CE.[100] El núcleo de esta nueva normativa es el artículo 89 del RGPD, que va acompañado de otras muchas referencias a lo largo de todo el texto que lo completan. Éstas se encuentran tanto en la parte del RGPD que incluye los criterios decisivos para su interpretación (considerandos), como en algunas disposiciones[101] específicas. Sobre la base de esos considerandos, cabe destacar algunas ideas preliminares.

En primer lugar, el considerando 157 afirma que, al acoplar la información de los registros, que incluyen diferentes tipos de datos correspondientes a una gran cantidad de individuos, los investigadores pueden obtener "nuevos conocimientos de gran valor en relación con afecciones médicas muy extendidas, como las enfermedades cardiovasculares, el cáncer y la depresión". Como consecuencia, "los resultados de la investigación pueden mejorar, ya que se basan en una población más amplia". Estas herramientas pueden contribuir a mejorar las políticas de investigación y, en consecuencia, la calidad de vida de la población. Estos beneficios hacen que el tratamiento de datos con estos fines por parte de los investigadores sea razonable, siempre que se garanticen los derechos de los sujetos. Se establece así una concepción de la investigación como un proceso que persigue un beneficio social, a corto, medio o largo plazo, considerado de forma muy amplia (mejora de la calidad de vida) pero, al mismo tiempo, limitando dicha actividad a esta finalidad concreta. Además, el considerando 159 precisa que "para responder a las especificidades del tratamiento de datos personales con fines de investigación científica, deben aplicarse condiciones específicas, en particular en lo que se refiere a la publicación o a la divulgación de otro tipo de datos personales en el marco de la investigación científica".

La segunda cuestión que debe abordarse es el carácter específico del consentimiento como requisito para su validez, que presenta algunas particularidades cuando la finalidad del tratamiento es la investigación científica. En efecto, el artículo 4 del RGPD establece que el consentimiento "es toda manifestación de voluntad del interesado, libre, específica, informada e inequívoca, por la que éste, mediante una declaración o una clara acción afirmativa, consienta el tratamiento de datos personales que le conciernen". Sin embargo, el considerando 33 afirma que "a menudo no es posible identificar plenamente la finalidad del tratamiento de datos personales con fines de investigación científica en el momento de la recogida de datos".

Sin embargo, es habitual que durante un proyecto surjan planteamientos no previstos inicialmente o que, al finalizarlo, las conclusiones abran las puertas a otros proyectos relacionados. Además, los investigadores y equipos suelen estar especializados en un área o línea de investigación desarrollada a partir de proyectos concretos, y los datos pueden seguir siendo útiles o necesarios durante largos periodos de tiempo[102]. Como respuesta, han surgido modelos institucionales -como los biobancos- que funcionan como intermediarios entre los sujetos y los investigadores. El objetivo de la recogida de estos datos es almacenarlos para cuando puedan ser necesarios, sin saber, en principio, qué proyecto de investigación, o

---

[100] Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (DO L 281 de 23.11.1995, p. 31).

[101] Véanse, *entre otros*: La letra b) del apartado 1 del artículo 5 para fines compatibles; la letra e) del apartado 1 del artículo 5 para la limitación del almacenamiento; la letra j) del apartado 2 del artículo 9 como excepción para el tratamiento de categorías especiales de datos; la letra b) del apartado 5 del artículo 14 para la transparencia y la información; la letra d) del apartado 3 del artículo 17 para el derecho de supresión; o el apartado 6 del artículo 21 para el derecho de oposición.

[102] A este respecto, véase también el artículo 5, apartado 1, letra e), del RGPD, que permite que los datos personales se conserven durante períodos más largos en la medida en que se traten únicamente "con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos de conformidad con el artículo 89, apartado 1".

proyectos, los tratarán. Ante esta realidad, el considerando 33 establece que "debe permitirse a los sujetos de los datos dar su consentimiento a determinadas áreas de la investigación científica", aunque "los sujetos de los datos deben tener la oportunidad de dar su consentimiento sólo a determinadas áreas de la investigación o partes de los proyectos de investigación en la medida en que lo permita la finalidad prevista". Por lo tanto, se permiten diferentes opciones y consentimientos, siempre que sean, como recuerda el considerando, "conformes a las normas éticas reconocidas para la investigación científica".

Un tercer punto que merece atención es el que figura en el considerando 50, que se refiere a la llamada compatibilidad de fines[103], es decir, al "tratamiento de datos personales para fines distintos de aquellos para los que se recogieron inicialmente". Se trata de un término que se utiliza en los casos en que los datos personales, destinados a ser utilizados con fines de investigación, se recogieron o trataron inicialmente con una finalidad distinta, pero pueden ser tratados legítimamente para otros fines nuevos (compatibles). Además, el tratamiento posterior con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos se consideran *ex lege* operaciones de tratamiento lícitas compatibles. Esto significa que no se requiere el consentimiento del interesado ni ninguna otra base jurídica para estos fines adicionales, en las condiciones que se describirán más adelante. Esta opción es de suma importancia para la investigación científica porque puede facilitar el acceso a una enorme cantidad de datos sin necesidad de volver a contactar con los interesados.

Por último, es necesario mencionar el considerando 53, que recoge la finalidad del RGPD relativa al establecimiento de condiciones armonizadas para el tratamiento de categorías especiales de datos personales con fines sanitarios (en particular, en el contexto de la gestión de los servicios y sistemas de asistencia sanitaria o social). Además, establece que "el Derecho de la Unión o de los Estados miembros debe prever medidas específicas y adecuadas para proteger los derechos fundamentales y los datos personales de las personas físicas", al tiempo que declara que "los Estados miembros deben estar autorizados a mantener o introducir otras condiciones, incluidas limitaciones, en relación con el tratamiento de datos genéticos, datos biométricos o datos relativos a la salud". Sin embargo, las medidas introducidas "no deberían obstaculizar la libre circulación de datos personales dentro de la Unión cuando esas condiciones se apliquen al tratamiento transfronterizo de dichos datos".

2.4.3 Nociones en el contexto del marco normativo de la UE

A. Noción de "fines de archivo en interés público"

Se entiende que los archivos de interés público son los de los organismos públicos o privados que conservan registros de interés público y que, en virtud del Derecho de la Unión o de los Estados miembros, tienen la obligación legal de adquirir, conservar, valorar, ordenar, describir, comunicar, promover, difundir y facilitar el acceso a los registros de valor permanente para el interés[104] público general. No obstante, no se aplica a los datos de personas fallecidas (véase "Datos personales", Parte II de estas Directrices, sección "Conceptos principales").

B. Noción de "investigación científica"

La investigación científica es un término demasiado amplio que, en general, se refiere a la búsqueda de conocimientos, a través de una determinada metodología, en cualquier área del conocimiento humano. El RGPD no incluye una definición de "investigación científica" como tal, pero introduce una serie de consideraciones que permiten definir sus principales

103 A este respecto, véase también el artículo 5.1.b) del RGPD.

104 Considerando 158 del RGPD.

características. En primer lugar, la investigación "científica" es diferente de los "fines de investigación histórica" y de los "fines estadísticos". Además, abarca diferentes campos, por ejemplo, la investigación en ciencias de la vida relacionada con la salud humana, pero también las ciencias sociales (considerandos 157 y 159). Debe aportar "beneficios", al menos potencialmente. Esta expectativa justifica un régimen único que permite excepciones y derogaciones de ciertos derechos (art. 89.2) [105]

En este marco, el RGPD realiza una interpretación amplia de la actividad científica, que incluye "el desarrollo y la demostración tecnológicos, la investigación fundamental, la investigación aplicada y la investigación con financiación privada" (considerando 159). Esta concepción amplia incluye los proyectos de investigación con resultados publicables y otros estudios analíticos, sin excluir la investigación financiada con fondos privados o por empresas comerciales con ánimo de lucro. Sin embargo, también contiene ciertos límites, unos criterios que permiten determinar hasta qué punto las excepciones previstas a lo largo del RGPD pueden aplicarse en un escenario de aumento de los procedimientos de análisis de datos. Sin embargo, el Reglamento sigue siendo ambiguo en cuanto a los parámetros que debe cumplir una actividad u operación de tratamiento para ser considerada "investigación científica". El SEPD, en un intento de arrojar algo de luz al respecto, ha aludido a los siguientes parámetros en su Dictamen Preliminar sobre protección de datos e investigación científica[106]:

- La actividad debe contribuir al aumento de los conocimientos (investigación científica en sentido estricto) o a la utilización de los conocimientos para la producción de dispositivos, materiales, servicios, procesos o productos (desarrollo tecnológico y demostración).
- La actividad debe desarrollarse bajo ciertos estándares de calidad (profesional, metodológica e institucional), "incluyendo la noción de consentimiento informado, responsabilidad y supervisión"[107].
- "La investigación se lleva a cabo con el objetivo de aumentar el conocimiento y el bienestar colectivo de la sociedad, en lugar de servir principalmente a uno o varios intereses privados". [108]

Según esta perspectiva, la investigación científica, a efectos del RGPD, abarca la actividad tanto de generación como de aplicación del conocimiento y excluye la actividad que no presenta una garantía de rigor en su desarrollo. Así, la investigación científica requiere que los proyectos de investigación "se establezcan de acuerdo con las normas metodológicas y éticas pertinentes del sector, de conformidad con las buenas prácticas".[109] Los procedimientos que permitan la adecuada evaluación de estos parámetros, que pueden variar de un caso a otro, representarán para el tratamiento de los datos en el sentido del artículo 89.1.

Es importante subrayar que la enseñanza [110]no puede considerarse una actividad científica, aunque esté destinada a la formación de profesionales de este sector. En consecuencia, dado que el RGPD no incluye ninguna mención al respecto, el tratamiento de datos con esta

105 Considerando 157 RGPD.

106 SEPD, Dictamen preliminar sobre la protección de datos y la investigación científica, 2020, p. 12. En: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_en.pdf Consultado: 15 de enero de 2020.

107 Ibid.

108 Ibid.

109 Comité Europeo de Protección de Datos (CEPD), Directrices 05/2020 sobre el consentimiento en virtud del Reglamento 2016/679, adoptadas el 4 de mayo de 2020, v1.1. p. 30. Disponible en: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf Accesible el 16 de septiembre de 2021.

110 "Enseñanza" no debe identificarse con "expresión académica" en el contexto del Art. 85 del RGPD.

finalidad está sujeto al régimen general, lo que puede dar lugar a numerosas disfunciones en la práctica. [111]

C. Noción de "investigación histórica"

El RGPD aplica esta descripción a los datos tratados con fines de investigación histórica. Se trata de un concepto amplio que incluye tanto la investigación histórica propiamente dicha como la investigación con fines genealógicos[112]. Sin embargo, no se aplica a la investigación realizada con datos de personas fallecidas.

D. Noción de "tratamiento con fines estadísticos"

Por fines estadísticos se entiende cualquier operación de recogida y tratamiento de datos personales necesaria para la realización de estudios estadísticos o para la obtención de resultados estadísticos[113]. Sin embargo, los datos resultantes deben ser datos no personales (datos agregados), y se requiere además que ni este resultado ni los datos personales se utilicen en apoyo de medidas o decisiones relativas a una persona física concreta.

Además, una vez más, el Derecho de la Unión o de los Estados miembros, dentro de los límites del RGPD, debe determinar la mayoría de los aspectos prácticos y particulares del tratamiento (qué datos se consideran contenido estadístico, el control del acceso y las medidas adecuadas para salvaguardar los derechos y libertades del interesado y para garantizar el secreto estadístico, etc.).

2.4.4 ¿Qué datos cubre el artículo 89?

Otro punto relevante de debate es la naturaleza de los datos cuyo tratamiento requiere garantías adecuadas y puede justificar excepciones y derogaciones a los derechos de los sujetos.

No cabe duda de que el artículo 89 comprende todas las categorías de datos personales, lo que incluye también el tratamiento de categorías especiales de datos personales, siempre que se cumplan las condiciones para el tratamiento de estos últimos.

Así, el uso secundario de los datos con fines de archivo, de investigación científica o histórica, o con fines estadísticos (art. 5), debe estar respaldado por las garantías mencionadas en el art. 89 cuando, por ejemplo, el análisis o el cruce con otros datos ponga de manifiesto información de carácter sensible. Por lo tanto, al aplicar el régimen del Art. 89, el contexto del tratamiento, sus implicaciones y la naturaleza de los datos revisten una importancia primordial.

2.4.5 Compatibilidad con el propósito

Según el artículo 5, apartado 1, letra b), el tratamiento posterior con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos es compatible incluso si los datos se recogieron inicialmente para otros fines diferentes (siempre que se apliquen medidas técnicas y organizativas que garanticen el respeto de los derechos y libertades del interesado). Sin embargo, sigue siendo objeto de debate si pueden aplicarse otras disposiciones, por ejemplo, la prueba de compatibilidad prevista en el artículo 6, apartado 4, del RGPD.

Sin embargo, en relación con las categorías especiales de datos, el artículo 9 (2) (j) menciona explícitamente que el tratamiento debe estar "basado en el Derecho de la Unión o de los

111 Véase, sobre la "expresión académica", el SEPD, p. 10.
112 Considerando 160 RGPD.
113 Considerando 162 RGPD.

Estados miembros, que será proporcional al objetivo perseguido, respetará la esencia del derecho a la protección de datos y establecerá medidas adecuadas y específicas para salvaguardar los derechos fundamentales y los intereses del interesado".

Este aparente problema jurídico requiere un esfuerzo interpretativo que podría resolver la cuestión de dos maneras. En primer lugar, dado que el artículo 5 no se refiere a categorías especiales de datos personales, podría entenderse que se limita a los casos en los que no se utiliza este tipo de información. Si se hablara de datos personales de estas categorías, se aplicaría el artículo 9, que es más específico.

La segunda solución se basa en una interpretación del artículo 5 simplemente como principios generales, y a la luz del considerando 50, que esboza una serie de condiciones para el uso secundario, que representan el requisito de un mayor autocontrol por parte del responsable del tratamiento, así como una "expectativa razonable" por parte del interesado de que este tratamiento secundario puede tener lugar. Además, el art. 6(4) establece una serie de criterios para determinar la compatibilidad de una operación de tratamiento con la finalidad (diferente) para la que se recogieron los datos personales, que también deben tenerse en cuenta en estos casos: "a) cualquier vínculo entre los fines para los que se han recogido los datos personales y los fines del tratamiento posterior previsto; b) el contexto en el que se han recogido los datos personales, en particular en lo que respecta a la relación entre los interesados y el responsable del tratamiento; c) la naturaleza de los datos personales, en particular si se tratan categorías especiales de datos personales, de conformidad con el artículo 9, o si se tratan datos personales relacionados con condenas e infracciones penales, de conformidad con el artículo 10; d) las posibles consecuencias del tratamiento posterior previsto para los interesados; e) la existencia de garantías adecuadas, que pueden incluir el cifrado o la seudonimización" (véase "Identificación", "Seudonimización" y "Anonimización" en la Parte II de estas Directrices, sección "Conceptos principales"). Por lo tanto, parece que los artículos 5, 6 y 9 deben leerse e interpretarse conjuntamente[114].

2.4.6 Cuestiones conceptuales: base jurídica del tratamiento.

Por lo que respecta a la base jurídica del tratamiento, es pertinente distinguir entre categorías de datos:

- Tratamiento de datos personales ("no sensibles"). Las bases jurídicas para el tratamiento son las establecidas en el artículo 6 del RGPD (véase "Legalidad, equidad y transparencia" en la sección "Principios" de la Parte II de estas Directrices). Esto significa que todo tratamiento de datos personales debe basarse necesariamente en alguna de las bases jurídicas previstas en el artículo 6, apartado 1:
  a) Consentimiento del interesado (art. 6.1 a).
  b) Contrato (art. 6.1 b).
  c) Obligación legal (art. 6.1 c).
  d) Intereses vitales (art. 6.1 d).
  e) Función pública o interés público (art. 6.1 e).
  f) Intereses legítimos (art. 6.1 f).
- Tratamiento de categorías especiales de datos personales ("datos personales sensibles"). El tratamiento de las categorías de datos incluidas en el artículo 9 está prohibido a menos que se identifique una base legítima específica de las que figuran en el apartado 2 del

114 SEPD, Dictamen preliminar sobre la protección de datos y la investigación científica, 2020, p. 23. En: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_en.pdf Consultado: 15 de enero de 2020.

artículo 9.[115] El artículo 9 requiere una legitimación adicional, que se suma a las del artículo 6. Entre estas bases legales, el tratamiento no está prohibido si, entre otras cosas.

a) "el interesado ha dado su consentimiento explícito al tratamiento de esos datos personales para uno o varios fines específicos, salvo que el Derecho de la Unión o de los Estados miembros disponga que el interesado no puede levantar la prohibición mencionada en el apartado 1". Artículo 9(2) letra a).
b) es "necesaria para fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, basados en el Derecho de la Unión o de los Estados miembros, que deberán ser proporcionales al objetivo perseguido, respetar la esencia del derecho a la protección de datos y prever medidas adecuadas y específicas para salvaguardar los derechos fundamentales y los intereses del interesado". [116]

Además, el artículo 9 (4) dice: "Los Estados miembros podrán mantener o introducir otras condiciones, incluidas limitaciones, con respecto al tratamiento de datos genéticos, datos biométricos o datos relativos a la salud". Sin embargo, esta posibilidad no implica que el contenido de la letra j) del apartado 2 del artículo 9 deba quedar sin efecto. Una vez más, los investigadores deberían pedir siempre consejo a sus DPD sobre el marco normativo nacional aplicable.

2.4.7 Tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos y derecho a la información

Cuando los datos personales no se hayan obtenido del interesado y el tratamiento se realice con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, el Reglamento prevé excepciones al derecho de información. En estrecha relación con los dos puntos anteriores, y para facilitar la disponibilidad de los datos para esos fines, el artículo 14, apartado 5, letra b), del RGPD establece que las disposiciones de los apartados 1 a 4 (que describen la información que el responsable del tratamiento debe transmitir al interesado) no se aplicarán cuando "el suministro de dicha información resulte imposible o suponga un esfuerzo desproporcionado, en particular para el tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, en las condiciones y con las garantías contempladas en el apartado 1 del artículo 89 o en la medida en que la obligación contemplada en el apartado 1 del presente artículo pueda hacer imposible o perjudicar gravemente la consecución de los objetivos de dicho tratamiento. En estos casos, el responsable del tratamiento adoptará las medidas adecuadas para proteger los derechos y libertades y los intereses legítimos del interesado, incluida la puesta a disposición del público de la información."

---

115 Comité Europeo de Protección de Datos (CEPD), Dictamen 3/2019 relativo a las preguntas y respuestas sobre la interacción entre el Reglamento sobre ensayos clínicos (RCE) y el Reglamento general de protección de datos (RGPD) (art. 70.1.b)) Adoptado el 23 de enero de 2019, pp. 8-9. En: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_opinionctrq_a_final_en.pdf Consultado: 20 de mayo de 2020.
Este documento describe varias posibilidades que combinan los artículos 6 y 9: Los motivos legítimos para el tratamiento pueden derivarse de las obligaciones legales del responsable del tratamiento y que entran en la base jurídica del artículo 6.1.c) en conjunción con el artículo 9.1.i); o el interés público en virtud del artículo 6.1.e) en conjunción con el artículo 9.2, i) o j); o los intereses legítimos del responsable del tratamiento en virtud del artículo 6, apartado 1, letra f), en relación con el artículo 9, apartado 2, letra j); o en circunstancias específicas, cuando se cumplan todas las condiciones, el consentimiento explícito del interesado en virtud del artículo 6, apartado 1, letra a), y del artículo 9, apartado 2, letra a).

116 Artículo 9(2)(j).

Por lo tanto, como puede deducirse de la literalidad de la disposición, no es necesario un desarrollo posterior por parte del Derecho de la Unión o de los Estados miembros para aplicar esta excepción.

2.4.8 Excepciones a determinados derechos de los interesados en virtud del artículo 89

El artículo 89, apartado 2, del RGPD establece: "Cuando se traten datos personales con fines de investigación científica o histórica o con fines estadísticos, el Derecho de la Unión o de los Estados miembros podrá establecer excepciones a los derechos contemplados en los artículos 15, 16, 18 y 21, con arreglo a las condiciones y garantías contempladas en el apartado 1 del presente artículo, en la medida en que dichos derechos puedan hacer imposible o perjudicar gravemente la consecución de los fines específicos, y dichas excepciones sean necesarias para el cumplimiento de dichos fines. "Junto con la letra b) 5del artículo 14, esta cláusula introduce varias excepciones relativas a los derechos de los interesados (véase la sección "Derechos de los interesados" en la Parte II de estas Directrices), a saber

- Derecho de acceso (artículo 15 del RGPD): Según el artículo 89, es posible limitar el derecho de acceso de los interesados. Esta limitación abarca tanto los datos personales tratados para la investigación como los datos personales obtenidos como resultado de los análisis o procedimientos desarrollados. En el ámbito biomédico, por ejemplo, se trata de los resultados obtenidos de exámenes o procedimientos corporales, análisis de sus muestras o datos, etc.

- Derecho de rectificación (artículo 16 del RGPD): El derecho a que se rectifiquen o completen los datos inexactos no tiene gran importancia en la investigación científica (puede ser más relevante, por ejemplo, en la investigación histórica). Tampoco lo es su limitación. La metodología de la investigación científica exige la exactitud y fiabilidad de la información que se maneja para que se obtengan conclusiones sólidas, por lo que redundará en su propio interés exigir dicha exactitud;

- Restricción del tratamiento (artículo 18 del RGPD): La restricción del tratamiento "significa el marcado de los datos personales almacenados con el fin de limitar su tratamiento en el futuro" (artículo 4, apartado 3, del RGPD). Los datos personales cuyo tratamiento se limita no se eliminan y se conservan para fines diferentes, pero no pueden utilizarse ni transferirse más allá de ese ámbito. En el marco de una investigación, el ejercicio de este derecho podría obstaculizar la continuidad de la investigación o la publicación de resultados en su primera fase (limitación de la continuidad de su uso). Por ello, esta excepción tiene sentido.

- Derecho de oposición (art. 21 del RGPD): El derecho de oposición permite al interesado cuyos datos personales están siendo tratados en virtud de cualquier fundamento jurídico distinto del consentimiento, oponerse al tratamiento. Esta posibilidad es la base de los llamados sistemas de exclusión voluntaria (en los que se presume el consentimiento para el uso de los datos con fines de investigación), y fundamental para los casos en los que no se requiere el consentimiento para el tratamiento (artículos 5 y 9 del RGPD). Plantear excepciones a este derecho tiene importantes consecuencias para la autonomía de los interesados, ya que puede implicar que los datos se utilicen en contra de su voluntad. Justificar estas excepciones como obstáculo que pueden representar para la investigación, sería bastante sencillo en cualquier caso en el que estos datos sean relevantes para la investigación.

Ejemplo: Investigación sobre enfermedades raras

La investigación sobre enfermedades raras suele basarse en datos personales obtenidos de un número bastante reducido de sujetos de datos (debido a la naturaleza pura de las enfermedades raras). Por lo tanto, si un número significativo de personas que participan en la investigación deciden ejercer sus derechos de restricción y/o de objeción, la representatividad y la fiabilidad de los datos de la investigación podrían verse significativamente socavadas como consecuencia. Además, los investigadores podrían enfrentarse a graves problemas en términos de publicación, ya que no podrían proporcionar esos datos al editor. Por lo tanto, en tales circunstancias, el responsable del tratamiento podría hacer uso de las excepciones a estos derechos establecidas en el artículo 89.

Los responsables del tratamiento deberán tener siempre presente que "cualquier excepción a estos derechos esenciales de los interesados deberá estar sujeta a un nivel de escrutinio especialmente elevado, en consonancia con las normas exigidas por el artículo 52, apartado 1, de la Carta". En consecuencia, las excepciones previstas en el artículo 89.2 del RGPD sólo son posibles si se cumplen las condiciones y las garantías exigidas en el artículo 89.1.

Además, en virtud del artículo 89, apartado 2, las excepciones sólo pueden aplicarse "en la medida en que" los derechos que se van a exceptuar "puedan hacer imposible o perjudicar gravemente la consecución de los fines específicos, y dichas excepciones sean necesarias para el cumplimiento de dichos fines".[117] Por último, los responsables del tratamiento deben considerar que "el hecho de que el establecimiento de medidas técnicas y organizativas para proporcionar acceso y otros derechos a las personas pueda requerir recursos financieros y humanos no es en sí mismo una justificación válida para establecer una excepción a los derechos de las personas en virtud del RGPD". [118]

Por último, por lo que respecta únicamente a los datos tratados con fines de archivo en interés público, el Derecho de la Unión o de los Estados miembros puede prever, además de las mencionadas, excepciones al derecho de notificación en materia de rectificación, supresión o limitación del tratamiento (artículo 19) y al derecho de portabilidad (artículo 20)[119]. Una vez más, esto requiere que el ejercicio de estos derechos pueda imposibilitar o dificultar gravemente la consecución de los fines específicos y que dichas excepciones sean, en consecuencia, necesarias para el cumplimiento de dichos fines.

Excepciones al derecho de supresión o al derecho al olvido

Según la letra d) del apartado 3 del artículo 17, este derecho no se aplicará en la medida en que el tratamiento sea necesario para fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos de conformidad con el apartado 1 del artículo 89, en la medida en que pueda hacer imposible o perjudicar gravemente la consecución de los objetivos de dicho tratamiento.

117 SEPD, Dictamen preliminar sobre la protección de datos y la investigación científica, 2020, p. 21. En: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_en.pdf Consultado: 15 de enero de 2020.

118 Dictamen del SEPD sobre las garantías y excepciones en virtud del artículo 89 del RGPD en el contexto de una propuesta de Reglamento sobre estadísticas agrícolas integradas, 2017. p.3. En: https://edps.europa.eu/sites/edp/files/publication/17-11-20_opinion_farm_statistics_en.pdf. Consultado: 17 de enero de 2020.

119 Véase el apartado 3 del artículo 89 del Reglamento.

Del mismo modo, las excepciones al derecho de supresión se aplicarán directamente, sin necesidad de que los Estados miembros las desarrollen.

2.4.9 Limitación de almacenamiento

Según el artículo 5, apartado 1, letra e), del RGPD, los datos personales deben "conservarse en una forma que permita la identificación de los interesados durante un período no superior al necesario" (véase el "Principio de limitación del almacenamiento" en la sección "Principios" de la Parte II de las presentes directrices). Sin embargo, el RGPD permite el almacenamiento durante períodos más largos si el único objetivo es la investigación científica (o el archivo en interés público, la investigación histórica o los fines estadísticos), siempre que los responsables del tratamiento puedan proceder a dicho tratamiento con una base jurídica adecuada (el almacenamiento implica el tratamiento de datos). "La intención del legislador parece haber sido disuadir del almacenamiento ilimitado incluso en este régimen especial, y previene contra la investigación científica como pretexto para un almacenamiento más prolongado con otros fines privados. En caso de duda, el responsable del tratamiento debe considerar si es conveniente una nueva base jurídica".[120]

Por lo tanto, los períodos de almacenamiento deben ser proporcionales a los objetivos del tratamiento. "Para definir los períodos de almacenamiento (plazos), deben tenerse en cuenta criterios como la duración y la finalidad de la investigación. Hay que tener en cuenta que las disposiciones nacionales pueden estipular también normas relativas al periodo de almacenamiento".[121]

2.4.10 Garantías adecuadas que deben adoptarse en virtud del apartado 1 del artículo 89

El apartado 1 del artículo 89 exige que se apliquen "garantías adecuadas" al tratamiento de datos personales con fines de investigación científica o histórica o con fines estadísticos, independientemente de cuál sea la base jurídica del tratamiento. El objetivo de estas garantías es asegurar el respeto del principio de minimización de los datos personales (véase la subsección "Principio de minimización" en la sección "Principios" dentro de la Parte II de estas Directrices. Así pues, el primer parámetro que debe analizarse es si se cumplen las condiciones propias del tratamiento de datos personales, es decir, el tratamiento de datos personales debe ser necesario para llevar a cabo esa investigación concreta. El apartado 1 del artículo 89 establece que las garantías adecuadas "deben reflejarse en medidas técnicas y organizativas", como la seudonimización. La seudonimización debe ir acompañada de otras disposiciones, en función de los riesgos de cada proyecto. Los responsables del tratamiento deben velar siempre por la aplicación de medidas técnicas y organizativas adecuadas destinadas a garantizar la protección de los derechos y libertades de los interesados. A continuación, se presentan algunos ejemplos posibles de dichas medidas o salvaguardias:

- Control del acceso a las bases de datos de forma que dicho acceso sólo se permita a personas autorizadas, para investigaciones aprobadas, con interés científico justificado, y solución informática implementada que permita un control auditable de los archivos de registro de acceso.

120 Comité Europeo de Protección de Datos (CEPD), Directrices 03/2020 sobre el tratamiento de datos relativos a la salud con fines de investigación científica en el contexto del brote de COVID-19. Adoptadas el 21 de abril de 2020, p. 10. En https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf (última visita: 23 de abril de 2020).

121 Ibidem, p. 10.

- Firma de un compromiso jurídicamente vinculante entre las partes, que incluye las condiciones del tratamiento: compromiso de confidencialidad y no identificación de los interesados, y uso de los datos para la finalidad específica autorizada.

- Aplicación de medidas de seguridad para garantizar la protección de la transferencia y el almacenamiento de datos en el destinatario.

- Garantizar la transparencia de la información proporcionada a los participantes.

- Seguimiento continuo de las condiciones de tratamiento a lo largo del tiempo, que podría adoptar la forma de medidas de transparencia (publicación y accesibilidad de las políticas de gestión de datos) y de previsiones a largo plazo (identificación de las obligaciones del responsable del tratamiento). En relación con este último punto, cabe destacar la necesidad de establecer compromisos claros de control de la gestión/tratamiento de los datos personales por parte de la institución que lleva a cabo la investigación y que podría encomendarse más específicamente al Comité de Ética de la Investigación (CEI) correspondiente.

- Establecimiento de un sistema de control externo al investigador que podría ser competencia del CEI correspondiente o de la dirección del centro de investigación, que debería participar en el citado acuerdo.

Además, los investigadores deben tener en cuenta que existen otros mecanismos previstos en el régimen general del RGPD que también introducen medidas adecuadas al tratamiento de datos con fines de investigación en el sentido del artículo 89.1, como las EIPD o la intervención de los DPD. Por último, es interesante mencionar que existen iniciativas para promover códigos de conducta y mecanismos de certificación internacionales que pueden armonizar estas salvaguardias.

2.4.11 **Más información**

- SEPD, Dictamen sobre las garantías y excepciones en virtud del artículo 89 del RGPD en el contexto de una propuesta de Reglamento sobre estadísticas agrícolas integradas, 2017. En: https://edps.europa.eu/sites/edp/files/publication/17-11-20_opinion_farm_statistics_en.pdf
- SEPD, Dictamen preliminar sobre la protección de datos y la investigación científica, 2020. En: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_en.pdf.
- Comité Europeo de Protección de Datos, Dictamen 3/2019 relativo a las preguntas y respuestas sobre la interacción entre el Reglamento sobre ensayos clínicos (RCE) y el Reglamento general de protección de datos (RGPD) (art. 70.1.b). Aprobado el 23 de enero de 2019. En: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_opinionctrq_a_final_en.pdf
- Comité Europeo de Protección de Datos, Directrices 03/2020 sobre el tratamiento de datos relativos a la salud con fines de investigación científica en el contexto del brote de COVID-19. Adoptadas el 21 de abril de 2020. En: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_en.pdf