ITI INVESTIGATE TO INNOVATE

GUÍA PARA EL CUMPLIMIENTO NORMATIVO EN LA INVESTIGACIÓN Y EXPERIMENTACIÓN CON INTELIGENCIA ARTIFICIAL Y TECNOLOGÍAS CONEXAS EN ESPACIOS DE INNOVACIÓN CON DATOS, CENTRADA EN PRIVACIDAD Y DATA GOVERNANCE

Lorenzo Cotino Hueso

Autor:

Lorenzo Cotino Hueso

Catedrático de Derecho Constitucional

Universitat de València

Edición y coordinación:

Óscar Valle Ballesteros

Daniel Sáez Domingo

Instituto Tecnológico de Informática

Revisión:

Nieves Ruiz Alberola

Instituto Tecnológico de Informática

GUÍA elaborada en el marco del proyecto VAIH: DIH en Inteligencia Artificial, financiado por la Agencia Valenciana de la Innovación con número de expediente INNACC00/19/030 en el programa de Acciones complementarias de impulso y fortalecimiento de la innovación.

ISBN: 978-84-09-31738-7

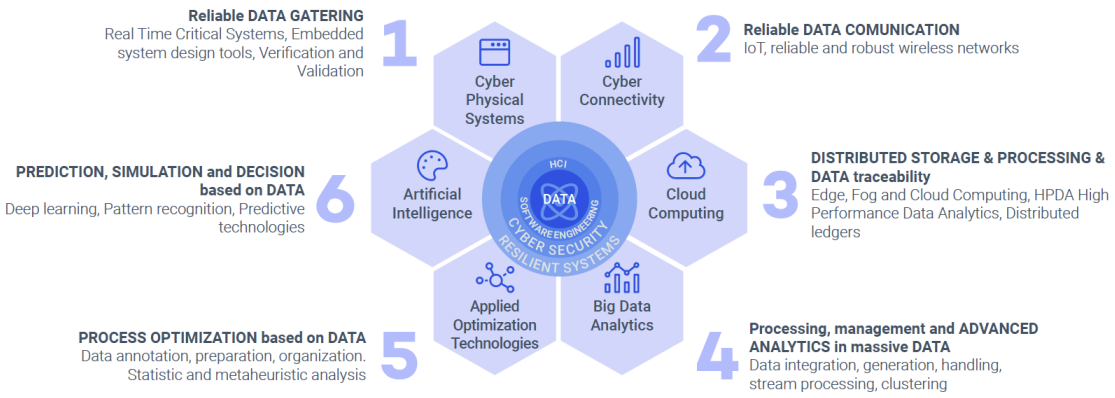
CONTENIDO GENERAL

ÍNDICE DETALLADO

I. ACERCA DE ITI Y SU DATA SPACE

El Instituto Tecnológico de Informática, ITI, es un Centro Tecnológico especializado en Investigación, Desarrollo e Innovación en Tecnologías de la Información y las Comunicaciones para para mejorar y mantener la posición competitiva de las empresas tecnológicas, generando y transfiriendo los conocimientos necesarios para la evolución de la industria y de la sociedad en general.

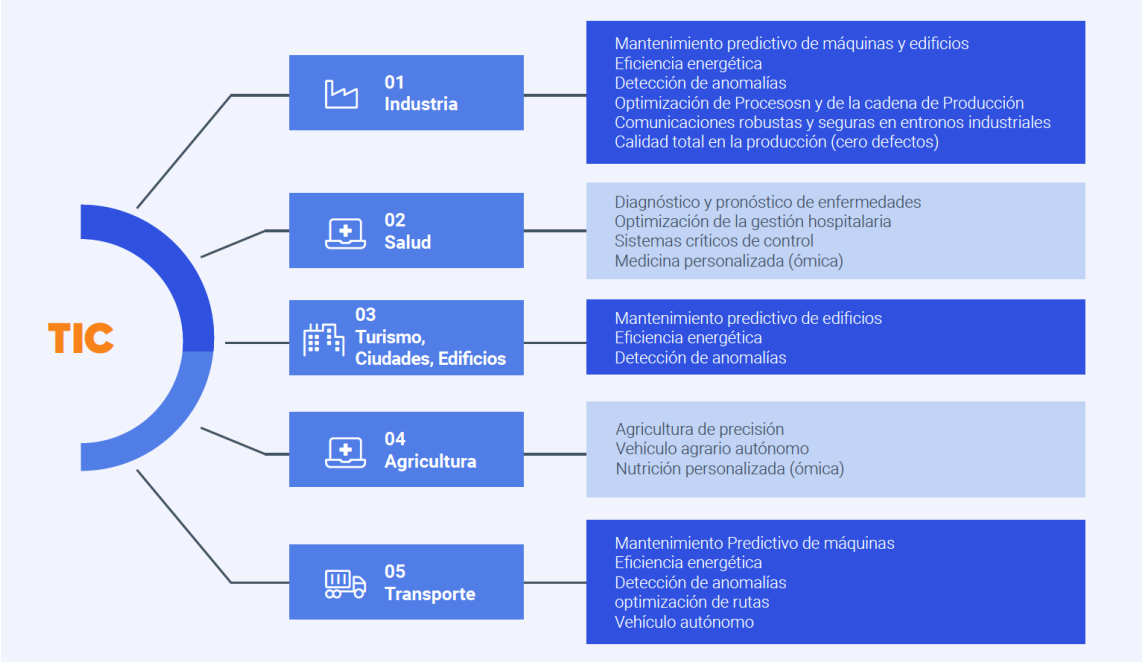
ITI es un centro de referencia a nivel nacional e internacional en la captación, comunicación y explotación de los datos de forma robusta, segura y eficiente para ayudar a la toma de decisiones en múltiples dominios de aplicación. Su actividad de I+D+I se enmarca en las siguientes áreas, totalmente alineadas con el programa Horizonte Europa, la Estrategia Española de Ciencia, Tecnología y de la Innovación, la Agenda Digital Europea, Española y de la Comunidad Valenciana y la Estrategia de Especialización Inteligente en investigación e Innovación de la Comunidad Valenciana (RIS3 CV):



Con el centro de gravedad en el Dato, ITI cuenta con un equipo humano de más de 230 tecnólogos, entre investigadores y técnicos, que centra su actividad en el conjunto de habilitadores digitales que permiten la captación del dato con precisión y fiabilidad (Sistemas Ciberfísicos), su comunicación (**Ciber conectividad**, Internet de las Cosas, …), su almacenamiento y procesamiento distribuido (Cloud/Edge Computing, Blockchain, …), la analítica en grandes cantidades (Big Data Analytics) o usando técnicas estadísticas y metaheurísticas (Sistemas de Optimización) y su predicción y simulación (Inteligencia Artificial), la interacción con los usuarios para obtener y mostrar información de forma efectiva (***Human Computer Interaction - HCI***), y su aplicación para conseguir sistemas más robustos (**Sistemas Resilientes**), todo ello con las capas horizontales de **Ingeniería de Software** que aporta Calidad al software desarrollado y **Ciberseguridad** para la obtención de sistemas informáticos más seguros.

Todas estas tecnologías son de aplicación a múltiples dominios, aunque en los que más focalizado está ITI son:

- **Industria manufacturera:** Es uno de los sectores con mayor peso en la economía de la región y a nivel nacional, contemplando sectores tradicionales (agroalimentario, cerámico, calzado, textil, …) como sectores más avanzados (automoción, bienes de equipo, …)
- **Salud:** Es el segundo sector por importancia en los trabajos realizados por ITI, incluyendo desde la mejora en la gestión de enfermedades y pacientes hasta la mejora en los equipos e instalaciones.
- **Turismo, ciudades y edificios:** Incluye los elementos incluidos en la ciudad, su gestión eficiente, inclusiva, personalizada y anticipativa.
- **Agricultura:** Uno de los sectores con mayor peso en España y con grandes oportunidades de digitalización, abordando aspectos como agricultura y ganadería de precisión y contribuyendo al ahorro de materias primas y mejora de la calidad de los productos.
- **Transporte:** Sector específico de transporte de mercancías.



Durante los últimos años, ITI ha puesto un gran esfuerzo en desarrollar las bases que sustenten **la Inteligencia Artificial y las tecnologías basadas en Datos en Europa,** aportando un liderazgo activo que se traduce en algunos hitos como los siguientes:

- **Miembro fundador (2104) de la asociación europea Big Data Value Association (BDVA, actualmente DAIRO), y líder del grupo de iSpaces** de dicha Asociación, que son espacios de experimentación con datos, infraestructuras y tecnologías de Big Data e Inteligencia Artificial.
- Líder del proyecto Europeo **EUHubs4Data - European Federation of Data Driven Innovation Hubs** que tiene como objetivo el **crear la mayor red europea de**

espacios de innovación en Datos, para lo cual cuenta con 12 nodos distribuidos en toda Europa que se ampliarán a lo largo de los 3 años de proyecto y que va a dar servicio a 42 experimentos de empresas.

- Líder del proyecto Europeo **DataPorts - A Data Platform for the Cognitive Ports of the Future**, que pretende convertir los puertos actuales en puertos inteligentes y cognitivos gracias a la creación de una Plataforma Industrial de Datos que facilite el intercambio de información de forma segura entre los agentes que forman parte de la cadena de valor.
- Participación activa en la creación de la **PPP "AI, Data and Robotics"**, con contribuciones a la definición de la **Agenda Estratégica de Investigación, Innovación y Despliegue de la Inteligencia Artificial** para la Comisión Europea.
- Líder del proyecto **AI4ES - Red de Excelencia Cervera en Tecnologías Habilitadoras Basadas en el Dato,** que tiene por misión *ser el referente español en I+D+I y transferencia* en Tecnologías Habilitadoras Digitales relativas a procesamiento y análisis inteligente de datos, principalmente *Inteligencia Artificial, incluyendo Machine Learning, Big Data y otras tecnologías basadas en datos,* con el fin de potenciar la economía basada en datos e inteligencia artificial.
- Líder del **grupo interplataformas en Big Data e Inteligencia Artificial** promovido por el Ministerio de Economía y que cuenta con la participación de más de 15 plataformas tecnológicas sectoriales en los ámbitos en los que España tiene una masa crítica elevada (Manufactura, Agua, Salud, Energía, …), además de la plataforma tecnológica PLANETIC, especializada en Tecnologías digitales.
- **Coordinador del Data Cycle Hub (DCH)**. El Data Cycle Hub, es un Digital Innovation Hub (DIH)[1], un ecosistema constituido por PYMES, grandes industrias, startups, administración pública, centros tecnológicos, aceleradores e inversores, etc... El mismo se ha puesto en marcha para fomentar la innovación basada en datos e inteligencia artificial en la Comunitat Valenciana. El DCH pretende consolidar un ecosistema que permita garantizar que cualquier empresa en la CV tenga acceso a conocimiento, tecnologías, infraestructuras, laboratorios, … en Digitalización, Big Data e Inteligencia Artificial, sea cual sea su sector y con un enfoque específico en las pymes y en la Administración pública.
- Miembro de la **AI Digital Innovation Hub Network**, a partir de la cual se ha establecido una alianza de colaboración con 24 DIHs en toda Europa.
- Co-líder de la puesta en marcha de la **TECH4CV** en 2018, 2019 y 2020, la alianza de **centros de competencias de la Comunitat Valenciana en tecnologías habilitadoras** para afrontar los retos de la nueva economía. A finales de 2020, esta alianza dio origen a la constitución de una nueva asociación denominada **Inndromeda, Alianza de Tecnologías Innovadoras de la Comunidad Valenciana**, que permitirá la

[1] https://ec.europa.eu/digital-single-market/en/digital-innovation-hubs-dihs-europe se trata de Centros de innovación digital, a modo de ventanillas únicas que ayudan a las empresas a ser más competitivas en sus procesos de negocio / producción, productos o servicios que utilizan tecnologías digitales. Los DIH brindan su experiencia técnica para que las empresas puedan "probar antes de invertir"

coordinación de diferentes tecnologías habilitadoras capaces de resolver las problemáticas presentes y futuras de las empresas de la Comunitat Valenciana, facilitando el camino hacia un modelo productivo basado en la Innovación, la Tecnología y el Conocimiento.

Como consecuencia de los hitos mencionados anteriormente, ITI ha consolidado su posición en el espacio nacional y europeo de datos y ha creado **su propio Data Space, que responde a una *infraestructura clave para soportar la evolución de la digitalización y el despliegue de las tecnologías de explotación de datos, posicionada como referencia regional y como nodo relevante en la esfera nacional e internacional***. *Sus principales recursos son:*

- Infraestructura Hardware
- Infraestructura SW y herramientas
- Algoritmos
- Datos
- Servicios

Este Data Space recibió el gold *label* como iSpace de la BDVA en 2020, y como tal proporciona:

- Un centro de experimentación especializado en Big Data e Inteligencia Artificial, que facilita y mejora ***la competitividad*** de las empresas mediante la transferencia de tecnologías en Big Data y conocimiento al mercado.
- Infraestructura técnica y legal con flujo controlado para la compartición de datos.
- Centro de datos confiable, conexión con data owners y acceso a datasets públicos y privados.
- Soporte, recomendaciones y buenas prácticas en todo o parte del flujo del dato.
- Mejora de decisiones en cuanto a inversión tecnológica (“test before invest”).

II. ÁREAS DE ESPECIAL OBJETO DE ATENCIÓN EN ESTA GUÍA

1. Objeto del documento

El presente documento pretende ser una Guía de buenas prácticas para el cumplimiento ético y normativo, centrada en privacidad y data governance respecto de plataformas o infraestructuras como el Data Space de ITI, como elemento clave para la compartición de datos y la experimentación en análisis avanzado de datos. De igual modo puede resultar de utilidad en ecosistemas como los referidos Digital Innovation Hub (DIH) que brindan innovación y experiencia e integran PYMES, grandes industrias, startups, administración pública, centros tecnológicos, aceleradores e inversores, etc.

El documento está basado en las necesidades particulares tanto de ITI como de las entidades que colaboran en su Data Space, especialmente por su actividad de investigación y experimentación, principalmente en las áreas de Big Data e Inteligencia Artificial, pero también en otras tecnologías habilitadoras digitales clave como los Sistemas Ciberfísicos, IoT, Cloud Computing y Plataformas de Computación de Alto Rendimiento u Optimización.

Aunque no exclusivamente, la presente guía se centra en el régimen de privacidad y protección de datos, puesto que en buena medida concentra la atención jurídica en las áreas de interés del Data Space de ITI. En todo caso, se pretende su disposición al público en general en tanto en cuanto se considera un recurso de interés para los proyectos y grupos de investigación, tan importantes, que utilizan inteligencia artificial y tecnologías conexas.

El presente documento tiene en cuenta el marco jurídico, si bien, pretende subrayar los elementos esenciales del mismo de modo comprensible y eficaz para quienes no son expertos jurídicos. Además del marco jurídico se ha concedido singular importancia a guías y documentos que en materia de protección de datos son referencia para Universidades y centros de investigación[2]. Se ha seguido de cerca la Guía de buenas prácticas en materia de Transparencia y Protección de Datos de la Conferencia de Rectores de las Universidades Españolas (CRUE)[3]. Se trata de un documento de

[2] Como se menciona en el apartado Normativas y protocolos internos, el Código de conducta UNED de 27 de junio de 2017 adaptado al Reglamento Europeo y otros previos no actualizados como el de la Universidad de Castilla-La Mancha (16 – noviembre – 2009 CT/0003/2004), Universidad de Oviedo de 2007. También entre otras, documentos como el de la U. Valencia (tampoco actualizado, Protocolo de actuación en materia de protección de datos).

[3] Septiembre de 2019, acceso en http://www.crue.org/Documentos%20compartidos/Publicaciones/Gu%C3%ADa%20de%20buenas%20pr%C3%A1cticas%20en%20materia%20de%20Transparencia%20y%20Protecci%C3%B3n%20de%20Datos/Gui%CC%81a%20de%20buenas%20pra%CC%81cticas_VD.pdf

referencia en el que han participado 54 instituciones asociadas a CRUE y las Secretarías Generales.

Asimismo, siendo especialmente relevantes como criterios de interpretación, se han seguido guías y documentos de referencia de las instituciones (Comité Europeo, OCDE, Consejo de Europa, Criterios de Inteligencia Artificial UE Alto grupo de expertos, Guías de la AEPD, y otras autoridades).

2. Conceptos convergentes. La inteligencia artificial y tecnologías conexas. De los algoritmos a la inteligencia artificial, sistemas de autoaprendizaje, robots. Big data e IOT

Según se ha adelantado el Data Space de ITI se focaliza en la innovación basada en datos e inteligencia artificial, en el ámbito de las tecnologías disruptivas y la digitalización principalmente a través de la experimentación en análisis avanzado de datos. Procede una aproximación a estos conceptos convergentes[4], con la advertencia de que para el ámbito jurídico y normativo es posible que los siguientes conceptos no siempre coincidan con los habituales en el ámbito tecnológico sobre el que han de proyectarse.

Un **algoritmo** puede concebirse como una secuencia de pasos para resolver un problema, comandos para que una computadora transforme un input en output. Uno o más se combinan e integran los programas informáticos desde hace décadas.

Por cuanto, a la **inteligencia artificial**, la Comisión Europea[5] en su Comunicación *IA para Europa* (COM (2018) 237 final, de 25 de abril de 2018 señala que "El término "IA" (IA) se aplica a los sistemas que manifiestan un comportamiento inteligente, pues son capaces de analizar su entorno y pasar a la acción –con cierto grado de autonomía– con el fin de alcanzar objetivos específicos." Tal **autonomía** se define como "capacidad para realizar tareas previstas en función del estado y la percepción actuales, sin intervención humana" (ap. 2.2). Norma ISO 8373 de 2012 sobre Robots y dispositivos robóticos (ver también Stanford University, 2016: 12-14). Los sistemas IA pueden ser deterministas, de modo que su respuesta queda totalmente predeterminada por los algoritmos, que pueden ser muy complejos. El sistema IA puede ser no determinista, esto es, capaz de dar respuestas

[4] Se sigue, Cotino Hueso, Lorenzo, "Riesgos e impactos del big data, la inteligencia artificial y la robótica y enfoques, modelos y principios de la respuesta del Derecho", BOIX PALOP, Andrés y COTINO HUESO, Lorenzo (coords.), *Monográfico Derecho Público, derechos y transparencia ante el uso de algoritmos, inteligencia artificial y big data RGDA Iustel*, nº 50, febrero 2019. Acceso en academia.edu

[5] Comisión Europea. (2018). IA para Europa. Comunicación de la Comisión al Parlamento europeo, al Consejo Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. COM(2018) 237 final{SWD(2018) 137 final} Bruselas, 25.4.2018, p. 1.

diferentes e imprevisibles en razón del aprendizaje y las circunstancias y entorno cambiante.

Se habla de "aprendizaje automático" o ***machine learning*** cuando los resultados de los algoritmos no dependen de lo que los humanos hayan especificado de antemano. Se suministran datos para que los sistemas y algoritmos identifiquen patrones y correlaciones, aprendan de ellos y generen nuevas relaciones, todo ello para hacer predicciones o recomendaciones. Mientras se ejecutan, los humanos no están controlando y en razón la naturaleza de la "caja negra", los resultados no siempre son intuitivamente explicables. El aprendizaje profundo o ***deep learning*** tiene aún menor intervención humana y está inspirado en el funcionamiento de redes neuronales de nuestro cerebro. Los grandes datos van pasando por distintas "capas" en la que se aplican reglas de aprendizaje, modelos para que pueda evaluar ejemplos e instrucciones para los resultados se vayan comparando y ajustando en cascada. El sistema aprende y utiliza lo aprendido para muy diversas finalidades.

En las *Normas de Derecho civil sobre robótica. Resolución del Parlamento Europeo*, de 16 de febrero de 2017 la **robótica** es la "capacidad de aprender de la experiencia y tomar decisiones cuasi independientes— ha hecho que estos robots se asimilen cada vez más a agentes que interactúan con su entorno y pueden modificarlo de forma significativa". Por su parte, la ISO 8373 de 2012 define robot como "mecanismo accionado programable en dos o más ejes con un grado de autonomía, que se mueve dentro de su entorno, para realizar las tareas previstas".

Relacionado con lo anterior, se hace también referencia a la **computación de alto rendimiento** (High performance Computing). Para resolver problemas complejos en ciencia, ingeniería o gestión que requiere el examen de grandes conjuntos de datos, se agrega una alta potencia de cálculo y se emplean tecnologías computacionales como los clústeres, los supercomputadores o la computación paralela.

Finalmente, y con carácter convergente, cabe hablar de un internet de las cosas robóticas ("Internet of Robotic Things, IoRT, Simoens)".

Pues bien, todas estas tecnologías convergentes "beben" del **big data o de los macrodatos**. Se habla de las "V" [6]: volumen, variedad, velocidad y valor, a las que se añaden entre otras, la veracidad[7]. El Big Data no sólo se refiere a grandes conjuntos de datos y las herramientas y procedimientos utilizados para manipular y analizar ellos, sino

[6] Gartner. (2012). *Emerging Market Analysis: IT*. Mexico, 2012 and beyond Gartner., julio, acceso completo en https://www.gartner.com/doc/2096518/emerging-market-analysis-it-mexico

[7] Puyol Moreno, Javier. (2014). "Una aproximación a Big Data", en *Revista de Derecho* UNED, núm. 14, págs. 471-505, p. 488. Acceso completo en Dialnet. De este autor, también, (2015). *Aproximación Jurídica y Económica al Big Data*, Tirant lo Blanch, Valencia.

también a un giro en el pensamiento computacional y la investigación (Boyd y Crawford[8]). Se da una necesaria convergencia del big data porque los sistemas computacionales son capaces de tratar, aprender, resolver problemas y tomar decisiones a partir de los grandes datos bajo un cambio de paradigma. La ingente acumulación de información y el big data es lo que ha permitido en los últimos años que vaya haciéndose efectivo el desarrollo de la IA.

En la también importante Resolución del Parlamento Europeo *de 14 de marzo de 2017, sobre las implicaciones de los macrodatos en los derechos fundamentales: privacidad, protección de datos, no discriminación, seguridad y aplicación de la ley* se afirma:"el concepto de macrodato se refiere a la recopilación, análisis y acumulación constante de grandes cantidades de datos, incluidos datos personales, procedentes de diferentes fuentes y objeto de un tratamiento automatizado mediante algoritmos informáticos y avanzadas técnicas de tratamiento de datos, utilizando tanto datos almacenados como datos transmitidos en flujo continuo, con el fin de generar correlaciones, tendencias y patrones (analítica de macrodatos)" (letra A).

Los datos pueden estar estructurados, semi-estructurados o no estructurados, lo cual es muy habitual. La más reciente normativa sigue haciendo referencia a la minería de datos. La misma se define como "«minería de textos y datos»: toda técnica analítica automatizada destinada a analizar textos y datos en formato digital a fin de generar información que incluye, sin carácter exhaustivo, pautas, tendencias o correlaciones".[9]

Procede asimismo hacer referencia al **Internet de las Cosas** (Internet of Things, IoT), o actualmente Internet del Todo, claramente vinculado con big data. En esencia implica la conectividad masiva de objetos sensorizados a través de internet, con la consiguiente generación también masiva de datos. Así, el Grupo del Artículo 29 de la UE en su Dictamen 8/2014 sobre la evolución reciente de la Internet de los objetos, 16 de septiembre de 2014 (p. 4) señala que el concepto de IoT "se refiere a una infraestructura en la que miles de millones de sensores incorporados a dispositivos comunes y cotidianos («objetos» como tales, u objetos vinculados a otros objetos o individuos) registran, someten a tratamiento, almacenan y transfieren datos y, al estar asociados a identificadores únicos, interactúan con otros dispositivos o sistemas haciendo uso de sus capacidades de conexión en red. Dado que la IO se basa en el principio del tratamiento amplio de los datos mediante estos sensores diseñados para comunicar datos de manera inadvertida e intercambiarlos de manera fluida, está estrechamente relacionada con las nociones de informática «generalizada» y «ubicua»."

La guía también se proyecta a ámbitos como los **Sistemas Ciberfísicos**. Con el mismo se hace referencia a un dispositivos o sistemas diseñados para controlar, monitorizar o interactuar con un proceso físico (por ejemplo, una red eléctrica, automóviles, sistemas

[8] Boyd D. y Crawford K. (2011). "Six Provocations for Big Data", *A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society*, p. 6 Acceso completo: https://ssrn.com/abstract=1926431

[9] Art. 2.2 Directiva (UE) 2019/790.

médicos, domótica, pilotos automáticos, etc.), sobre la base de algoritmos basados en computación y estrechamente integrados con Internet.

Uno de los denominadores comunes de todas las tecnologías convergentes mencionadas es el acceso y tratamiento de enormes cantidades de datos o big data a través de sistemas informáticos y tecnológicos muy avanzados. Como se verá, en algunos casos dichos datos son datos personales, lo cual atrae una especial atención jurídica y la exigencia de diversas obligaciones. De ahí el especial enfoque en privacidad y protección de datos.

III. ¿QUÉ NORMAS SE APLICAN?

1. Concurrencia de normativa, además de protección de datos

El tratamiento y manejo de datos, información y conocimiento y especialmente por medios digitales se da ya de manera casi *natural* en todos los sectores y por supuesto en los sectores tecnológicos 4.0. Y siempre que se trate de datos personales se aplicará casi por defecto el régimen de la protección de datos. De hecho, en muchas ocasiones, será casi el único régimen jurídico aplicable. Es por ello que esta guía se centra y tiene singular enfoque en privacidad y protección de datos.

Ahora bien, sobre la misma realidad de la gestión y tratamiento de datos, pueden concurrir y superponerse diversas normas de ámbitos más o menos afines. Los mismos no son objeto propio de este documento, pero hay que tener en cuenta.

Normativa de transparencia

Entre otras, cabe tener en cuenta la **normativa de transparencia**, que incluye obligaciones de facilitar información en las webs institucionales o cuando la solicita un ciudadano. Los sujetos privados pueden ser objeto de esta normativa especialmente cuando reciban subvenciones, sean partes de contratos o convenios públicos. Asimismo, mucha información de interés para la investigación puede proceder de esta información pública. Así, hay que tener especialmente en cuenta la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno . Así, para la Comunidad Valenciana hay que tener en cuenta la Ley 2/2015, de 2 de abril, de Transparencia, Buen Gobierno y Participación Ciudadana de la Comunitat Valenciana. Esta ley valenciana ha sido desarrollada por el Decreto 105/2017, de 28 de julio, del Consell.

Reutilización

La información pública puede ser muy importante como materia prima para la investigación, las bases de datos y, en general, para extraerle valor añadido con su **reutilización**. A este respecto hay que tener especialmente en cuenta la Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público. Esta norma ha sido actualizada en varias ocasiones y pronto habrá de ser reformada para recibir la muy reciente Directiva (UE) 2019/1024, de 20 de junio de 2019.

Normativa de datos no personales

La información y datos pueden no ser relativos a personas físicas, esto es, **datos no personales**. Además de la protección de los mismos como activo o propiedad, hay que tener en cuenta el reciente Reglamento (UE) 2018/1807 del Parlamento Europeo y del Consejo, de 14 de noviembre de 2018, relativo a un marco para la libre circulación de datos no personales en la Unión Europea, mediante el establecimiento de normas relativas a los requisitos de localización de datos, la disponibilidad de los datos para las autoridades competentes y la portabilidad de datos para los usuarios profesionales.

Normativa de propiedad intelectual

De especial importancia para la investigación, así como para la protección especial de sistemas y programas informáticos, incluso en su caso para los datos que manejen las bases de datos o los algoritmos que se desarrollen, es la **normativa de propiedad intelectual**. Así, cabe seguir el Texto refundido de la Ley de Propiedad Intelectual. Como se señala en el apartado "¿Qué derechos o propiedad tiene la entidad investigadora sobre el big data y sus algoritmos?", de particular interés (art. 12 - Colecciones. Bases de datos-, art. 34 - Artículo 34. Utilización de bases de datos por el usuario legítimo y limitaciones a los derechos de explotación del titular de una base de datos-, arts. 133-137, sobre Derecho "sui generis" sobre las bases de datos). Recientemente se ha aprobado en la UE la Directiva (UE) 2019/790 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, sobre los derechos de autor y derechos afines en el mercado único digital y por la que se modifican las Directivas 96/9/CE y 2001/29/CE. Esta norma debe incorporarse con regulación española a nuestro ordenamiento jurídico.

Normativa de secretos

Según se explicará, en la actualidad los algoritmos e incluso las bases de datos sólo cuentan corporativamente con la protección de la Ley 1/2019, de 20 de febrero, de Secretos Empresariales, que transpone la Directiva 2016/943/UE

Asimismo, la protección del Know-How, como secreto industrial, está recogido en la Ley de Competencia Desleal y en el Código Penal (artículos 278 y ss.).

Normativa penal

La información y los datos en sistemas informáticos son un valor y activo de las organizaciones protegido frente a ataques, robos, intrusiones, etc. En este sentido hay que tener en consideración la normativa penal. Así, en particular hay que centrar la atención en los Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio, con especial atención a los delitos de los artículos 197-201 (acceso y revelación de secretos, vulneración de seguridad informática, intercepción,). También de especial interés son los delitos de daños a programas o datos informáticos (art. 264), obstaculización o interrupción de sistema informático (art. 264 bis), entre otros delitos.

Normativa de seguridad y ciberseguridad

Cabe remitir al Código de Ciberseguridad (BOE). Entre otras normas, cabe también tener en cuenta el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, exigible a los servicios esenciales y de los servicios digitales, que además establece un sistema de notificación de incidentes. Y muchas veces en paralelo a la normativa de protección de datos para el sector público hay que tener en cuenta el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

2. Marco normativo de protección de datos y privacidad

El régimen de protección de datos en el ámbito universitario y de investigación viene determinado por una variada normativa española y de la UE. Es un derecho fundamental

reconocido por tratados internacionales (en especial, art. 8 CEDH, Convenio n. 108 del Consejo de Europa, de 28 de enero de 1981, actualizado en 2018), la Carta de derechos fundamentales de la UE (Artículos 7 y 8) y por nuestra Constitución (art. 18. 4º CE), si bien la regulación general básica viene establecida por una Reglamento europeo que se aplica directamente a los estados de la UE. No obstante, este reglamento hay que complementarlo con la legislación española, en particular la Ley Orgánica 3/2018, de 5 de diciembre "adapta" el reglamento europeo a España. El jurista necesita tener en cuenta conjuntamente estas dos normas generales de protección de datos.

En buena medida, la normativa es la siguiente, de fácil seguimiento Código BOE de protección de datos.

- Constitución Española. Art. 18.4
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Ley Orgánica 6/2001, de 21 de diciembre, de Universidades modificada por Ley Orgánica 4/2007, de 12 de abril (arts. 57, 62 y Disposición adicional 21).
- Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público (Artículos 3, 6, 133, 346 y disposiciones adicionales 15ª, 16ª y 25ª).
- Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público, modificada por Ley 18/2015, de 9 de julio y pendiente de incorporar la nueva Directiva de 2020.
- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- Ley Orgánica 1/1982, de 5 de mayo, sobre protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas
- Ley 9/2014, de 9 de mayo, General de Telecomunicaciones
- Ley 59/2003, de 19 de diciembre, de firma electrónica
- Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico

Imagen del Código de protección de datos del BOE.

Para el ámbito penal y de justicia hay que tener en cuenta la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y la libre circulación de dichos datos.

La privacidad de las comunicaciones electrónicas está regulada por la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas) fue modificada mediante la Directiva 2009/136/CE, de 25 de noviembre de 2009.

En la actualidad se está examinando la nueva propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas y por el que se derogaría la Directiva 2002/58/CE (Reglamento sobre la privacidad y las comunicaciones electrónicas).

3. Normativas y protocolos internos en organismos de investigación

Sin perjuicio de la normativa de privacidad y protección de datos a aplicar, las propias organizaciones pueden generar normas internas, de funcionamientos, protocolos que sean relevantes para la protección de datos.

En el ámbito universitario en el que muchas veces se desarrollan las investigaciones, cabe destacar algunas adecuaciones normativas. En particular el Código de conducta de

protección de datos de carácter personal de la universidad nacional de educación a distancia (UNED)[10], adaptado al Reglamento Europeo[11].

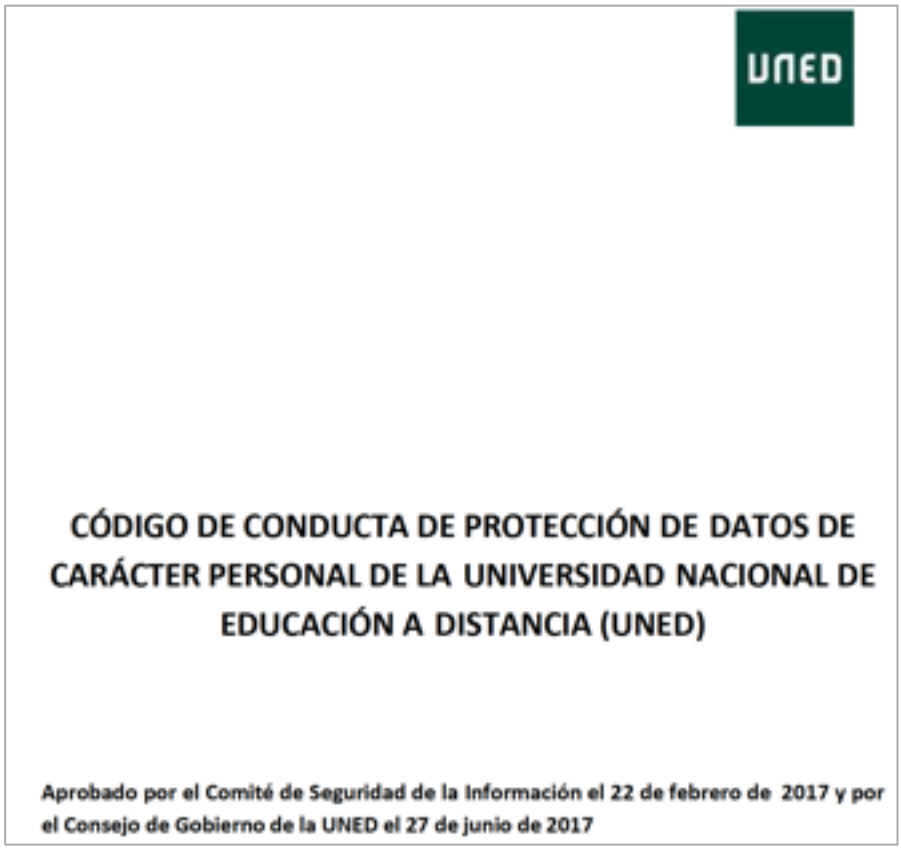


Imagen del Código de conducta de protección de datos de la UNED

Previos al RGPD, el Código de conducta de protección de datos personales en la Universidad de Castilla-La Mancha (16 – noviembre – 2009 CT/0003/2004) o el Código de buenas prácticas para la protección de datos de la Universidad de Oviedo de 2007[12]. En la U. Valencia, también con relación a la anterior normativa, Protocolo de actuación en materia de protección de datos[13].

Además de estas adaptaciones generales, que no son las habituales, es de especial interés tener en cuenta la normativa o adaptación interna a cuestiones particulares que

[10] Aprobado por el Comité de Seguridad de la Información el 22 de febrero de 2017 y por el Consejo de Gobierno de la UNED el 27 de junio de 2017.

[11] Aprobada, su adaptación, por el Consejo de Gobierno de la UNED el 30 de abril de 2019.

[12] Aprobado por Consejo de Gobierno de 21 de diciembre de 2007. BOPA de 15 de febrero de 2008, corrección de errores en BOPA 26 de marzo de 2008

[13] https://www.uv.es/fatwireed/userfiles/file/protocoloactuacionprotecciondatos.doc

puede haber en la propia organización. Así, por ejemplo, hay que tener en cuenta si la propia organización tiene adoptados reglamentos internos, normativas, e incluso procedimientos, protocolos o circulares a tener en cuenta. Asimismo, el incumplimiento de dichas normas puede generar responsabilidades internas.

Como más adelante se analizará, la normativa y procedimientos internos pueden ser especialmente relevantes al fijar procedimientos y responsabilidades dentro de la organización. En este punto, entre los relativamente recientes y completos del ámbito universitario, puede mencionarse el **Reglamento del registro de actividades de tratamiento de la Universitat Politècnica de València**[14] de 2019 que regula el régimen interno para la Autorización de la actividad de tratamiento (Titulo II); el registro de actividades de tratamiento (Titulo III) y las Obligaciones de los responsables internos del tratamiento (Titulo IV).

Muchas veces estas normas internas son la forma concreta de facilitar el cumplimiento normativo. Por ejemplo, puede haber normas sobre correo interno, uso de los sistemas de información, destrucción de documentos en papel, protocolos para dar de baja dispositivos hardware, bajas o altas de usuarios, con acceso a determinados datos, gestión de incidentes[15]. Asimismo, por ejemplo, Protocolo para el cumplimiento de la normativa de protección de datos en la realización de Prácticas Externas y Trabajos Fin de Estudios[16]

4. Derecho "blando" de las instituciones y autoridades de protección de datos

Más allá de la normativa y normativa interna, diversas instituciones especializadas en materia de protección de datos generan documentos que podemos calificar de *Derecho blando*. No se tratan de normas jurídicas obligatorias o *duras*. Sin embargo, se trata de documentos emitidos por las autoridades que controlan el cumplimiento de la normativa de protección de datos. Es por ello, que en buena medida lo que afirman tales documentos acaba siendo la forma de interpretar correctamente las normas. Ello tiene especial importancia en ámbitos especialmente innovadores respecto de los que las normas no son concretas y se generan conflictos y dudas.

[14] Aprobado por el Consejo de Gobierno de 16 de abril de 2019, Butlletí Oficial de la Universitat Politècnica de València Núm. 125 17/04/2019.
http://www.upv.es/contenidos/DPD/info/1074919normalc.html

[15] Al respecto, puede seguirse muchos ejemplos en el texto y anexos del Código de conducta la UNED mencionado.

[16] https://www.uv.es/farmadoc/TFG/Protocolo_proteccion_datos_TFG_PE.pdf

Directrices, dictámenes y documentos del Comité Europeo de Protección de datos y del –extinto- Grupo de Trabajo del artículo 29 y desde la UE

GRUPO DE TRABAJO DEL ARTÍCULO 29

El Grupo de Trabajo del artículo 29 (GT Art. 29) es el grupo de trabajo independiente formado por las autoridades de protección de datos de los miembros de la UE y el Supervisor Europeo de Protección de datos. En este órgano se aúnan criterios de aplicación de la normativa y se elaboran dictámenes, estudios, informes, etc. Pese a que interpretara la normativa anterior, sus dictámenes e informes siguen siendo la referencia en muchas de las materias[17].

Desde 2018, con el RGPD, dejó paso al nuevo Comité Europeo de Protección de Datos (CEPD)[18]. El mismo establece las directrices generales de la legislación europea de protección de datos para dar una interpretación coherente. Para ello proporciona orientaciones (incluidas directrices, recomendaciones y buenas prácticas). Puede dictar resoluciones vinculantes para las autoridades nacionales de supervisión para garantizar una aplicación coherente de la normativa.

[17] Puede accederse a más de cien estudios, dictámenes e informes (muchos de ellos en español en) https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm

[18] https://edpb.europa.eu/about-edpb/about-edpb_es

Del G 29 cabe destacar ahora por su interés:

- Directrices del Grupo de Trabajo del Artículo 29 (WP 259) sobre el consentimiento regulado en el RGPD.
- Directrices sobre la toma de decisiones y la elaboración de perfiles individuales automatizados a los efectos del Reglamento 2016/679, WP251rev.01.
- Dictamen 02/2016, del Grupo de Trabajo del Articulo (WP 239), relativo a datos personales para fines de transparencia en el sector público.
- Directrices sobre notificación de incumplimiento de datos personales en virtud del Reglamento 2016/679, WP250 rev.01.
- Directrices sobre el derecho a la portabilidad de datos en virtud del Reglamento 2016/679, WP242 rev.01.
- Directrices sobre la evaluación del impacto de la protección de datos (DPIA) y determinar si el procesamiento es "probable que genere un alto riesgo" a los efectos del Reglamento 2016/679, WP248 rev.01.
- Directrices sobre oficiales de protección de datos ('DPD'), WP243 rev.01.
- Pautas para identificar la autoridad supervisora principal de un controlador o procesador, WP244 rev.01.
- Documento de posición sobre las excepciones a la obligación de mantener registros de las actividades de procesamiento de conformidad con el Artículo 30 (5) del RGPD.

También de especial interés.

- Dictamen 06/2014, del Grupo de Trabajo del Artículo 29 (WP 217), relativo al concepto de interés legítimo.
- Dictamen 05/2014, del Grupo de Trabajo del Artículo 29 (WP 216), relativo a técnicas de anonimización.
- Dictamen 01/2014, del Grupo de Trabajo del Artículo 29 (WP 211), relativo a la aplicación de los conceptos de necesidad y proporcionalidad.
- Dictamen 03/2012, del Grupo de Trabajo del Artículo 29 (WP 193), relativo al desarrollo de las tecnologías biométricas.
- Dictamen 15/2011, del Grupo de Trabajo del Artículo 29 (WP 187), relativo a la definición de consentimiento.
- Dictamen 04/2007, del Grupo de Trabajo del Artículo 29 (WP 136), relativo al concepto de dato personal.
- Documento de trabajo del Grupo del Artículo 29 (WP 104), relativo a la relación entre protección de datos y derecho de propiedad intelectual.
- Documento de trabajo del Grupo del Artículo 29 (WP 67), relativo a videovigilancia.
- Documento de trabajo del Grupo del Artículo 29 (WP 55), relativo a la vigilancia de las comunicaciones electrónicas en el trabajo.

- Alguno de los documentos de especial interés del Comité Europeo[19].
- Escudo de privacidad UE - EE. UU.
- Declaración EDPB 3/2019 sobre una regulación de privacidad electrónica.
- Opinión 3/2019 sobre las preguntas y respuestas sobre la interacción entre el Reglamento de ensayos clínicos (CTR) y el Reglamento general de protección de datos (GDPR) - 23/01/2019.
- Declaración de EDPB sobre ePrivacy - 25/05/2018.
- Directrices 4/2019 sobre el Artículo 25 Protección de datos por diseño y por defecto - versión para consulta pública.
- Directrices 3/2019 sobre el procesamiento de datos personales a través de dispositivos de video: versión para consulta pública.
- Recomendación 01/2019 sobre el proyecto de lista del Supervisor Europeo de Protección de Datos con respecto a las operaciones de procesamiento sujetas al requisito de una evaluación de impacto de protección de datos (Artículo 39.4 del Reglamento (UE) 2018/1725).
- Directrices 2/2019 sobre el procesamiento de datos personales en virtud del Artículo 6 (1) (b) GDPR en el contexto de la prestación de servicios en línea a los interesados: versión adoptada después de consulta pública.
- Directrices EDPB 3/2018 sobre el alcance territorial del GDPR (artículo 3) - versión adoptada después de consulta pública.
- Directrices EDPB 1/2018 sobre certificación e identificación de criterios de certificación de conformidad con los artículos 42 y 43 del Reglamento - versión adoptada tras consulta pública.

Durante su primera reunión plenaria, la Junta Europea de Protección de Datos aprobó las Directrices WP29 relacionadas con el GDPR.

En febrero 2020[20] la Comisión Europea adoptó su *Libro Blanco sobre la Inteligencia Artificial, un enfoque europeo para la excelencia y la confianza,* acompañado de un importante anexo que ha marcado la política futura en la materia. Como uno de los reflejos del mismo, el Parlamento Europeo en otoño 2020 ha difundido un "Marco de los

[19] Acceso a documentos:

https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en

https://edpb.europa.eu/node/28

[20] COMISIÓN EUROPEA (2020 a). *Libro Blanco. Sobre la Inteligencia Artificial - Un enfoque europeo para la excelencia y la confianza,* COM (2020) 65 final, Bruselas, 19.2.2020. https://op.europa.eu/es/publication-detail/-/publication/aace9398-594d-11ea-8b81-01aa75ed71a1

aspectos éticos de la inteligencia artificial, la robótica y las tecnologías conexas", que incluye la Propuesta de Reglamento[21].

Igual que respecto del "Régimen de responsabilidad civil en materia de inteligencia artificial"[22], también con propuesta regulatoria.

"Para una IA 'made in Europe' un principio clave será el de **'ética por diseño'** según el cual los principios éticos y legales, conforme al Reglamento general de protección de datos, el cumplimiento de la ley de competencia, la ausencia de sesgo de datos se implementa desde el inicio del proceso de diseño." (Comisión Europea, 2018 b): 5-9 y 19-21).

Agencia Española de Protección de Datos

La Agencia Española de Protección de Datos es la autoridad independiente de nivel estatal, como función principal tiene la de vigilar y controlar el cumplimiento de la normativa de protección de datos por el sector público y privado. Asimismo, elabora informes y estudios de especial interés.

[21] Reglamento sobre los principios éticos para el desarrollo, el despliegue y el uso de la inteligencia artificial, la robótica y las tecnologías conexas. Resolución del Parlamento Europeo, de 20 de octubre de 2020, con recomendaciones destinadas a la Comisión sobre un marco de los aspectos éticos de la inteligencia artificial, la robótica y las tecnologías conexas (2020/2012(INL)).

Acompañado del extenso studio EPRS, European Parliamentary Research Service (Tatjana Evas), *European framework on ethical aspects of artificial intelligence, robotics and related technologies*. European added value assessment, September 2020.

[22] Resolución del Parlamento Europeo, de 20 de octubre de 2020, con recomendaciones destinadas a la Comisión sobre un régimen de responsabilidad civil en materia de inteligencia artificial (2020/2014(INL)).

Al momento de cerrarla revisión de esta Guía la AEPD ha destacado con la Guía Requisitos para auditorías de tratamientos de datos personales que incluyan Inteligencia Artificial, de enero 2021, realizada bajo el importante documento se encuadra en lo propuesto en la Guía de Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial de febrero 2020.

Guías de la AEPD sobre Inteligencia Artificial.

Entre sus documentos cabe destacar ahora[23]:

- Listado de elementos para el cumplimiento normativo Guía para responsables del tratamiento
- Guía para el cumplimiento del deber de informar
- Directrices para la elaboración de contratos entre responsables y encargados del tratamiento
- Guía para el ciudadano Conoce tus derechos
- Guía práctica de análisis de riesgos para el tratamiento de datos personales
- Guía práctica para las evaluaciones de impacto en la protección de datos personales
- Guía para la gestión y notificación de brechas de seguridad
- Guía para clientes que contraten servicios de Cloud Computing
- Orientaciones para prestadores de servicios de Cloud Computing

[23] Acceso sencillo en https://www.lopdencastellon.com/manuales-aepd-rgpd/

- Guía big data AEPD
- Guía para el responsable para el cumplimiento RGPD
- Guía para el cumplimiento del deber de informar de la AEPD y las agencias catalana y vasca.
- Guía cookies
- Orientaciones protección de datos reutilización
- Guía evaluación de impacto de protección de datos
- Guía cumplimiento RGPD
- Orientaciones y garantías procesos anonimización
- Estudio de impacto Guía eipd
- Resulta de especial interés la Guía EIPD APDCAT de la autoridad catalana
- Nota técnica "La K-anonimidad como medida de la privacidad".
- Orientaciones y garantías en los procedimientos de anonimización de datos personales.
- Guía sobre el uso de videocámaras para seguridad y otras finalidades.
- Orientación para la aplicación provisional de la Disposición Adicional Séptima de la LO 3/2018.

Guías de la AEPD

5. Los estándares o “normas” ISO

El RGPD hace referencia a los códigos de conducta y certificación artículos 40 a 43.

Aunque no son normas “oficiales” por cuanto provengan del Estado o de organizaciones internacionales públicas, son muy relevantes en el sector los estándares internacionales y en particular las normas ISO (International Organization for Standardization), e IEC (International Electrotechnical Comission). Con las mismas se puede para garantizar que los productos o servicios ofrecidos por dichas organizaciones cumplen con los objetivos de cada norma y sirven para acreditar niveles de cumplimiento garantizando a interesados y terceros un tratamiento de seguridad y protección de datos adecuado.

A través de esta normativa se estandarizan normas tanto para organizaciones públicas o privadas a nivel internacional. Ahora bien, en principio son normas de asunción voluntaria. No obstante, hay casos en los que la propia normativa “oficial” afirma que hay que cumplir con determinados estándares.

6. Normativa específica investigación biomédica

La presente guía, aunque hace referencias al marco jurídico de la investigación y la protección de datos, no puede abarcar de modo concreto el ámbito de la investigación biomédica. Se trata de un ámbito específico que requiere un tratamiento específico y, de hecho, cuenta con un marco jurídico particular que debe integrarse con la normativa

reguladora general sanitario[24]. A esta normativa cabe añadir incluso la específica normativa autonómica[25] (en el caso de la C. Valenciana, la Ley 10/2014, de Salud de la Comunitat Valenciana).

En cualquier caso, cabe recordar la normativa e instrumentos básicos a tener en cuenta:

- Art 89 y 9 RGPD
- Disposición Adicional 17 Ley orgánica 3/2018 y Disposición transitoria 6ª.
- Ley 14/2007, de 3 de julio, de Investigación Biomédica.
- Real Decreto 1716/2011, de 18 de noviembre, por el que se establecen los requisitos básicos de autorización y funcionamiento de los biobancos con fines de investigación biomédica y del tratamiento de las muestras biológicas de origen humano, y se regula el funcionamiento y organización del Registro
- Nacional de Biobancos para investigación biomédica.
- Ley 14/2011, de 1 de junio, de la Ciencia, la Tecnología y la Innovación.
- Real Decreto Legislativo 1/2015, de 24 de julio, por el que se aprueba el texto refundido de la Ley de garantías y uso racional de los medicamentos y productos sanitarios.
- Ley 21/2000, de 29 de diciembre, sobre los derechos de información concerniente a la salud y la autonomía del paciente, y a la documentación clínica.
- Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica

Y como interpretación del marco jurídico

- Dictámenes emitidos recientes por la Autoridad Catalana de Protección de Datos en los que se analiza el régimen establecido por la Disposición Adicional 17 Ley orgánica 3/2018, para el tratamiento de datos de salud en el marco de la investigación:
- Dictamen Autoridad Catalana de Protección de Datos CNS 15/2019. el tratamiento de datos seudonimizados con finalidades de investigación y base de legitimación
- Dictamen Autoridad Catalana de Protección de Datos CNS 18/2019. analiza otros aspectos de la Disposición Adicional 17
- Dictamen 3/2019, sobre “Preguntas y Respuestas sobre la interrelación entre la regulación de ensayos clínicos y el RGPD” de 23 de enero de 2019, del Comité Europeo de Protección de Datos.
- Informe 073667/2018 AEPD https://www.aepd.es/informes/juridicos/
- https://www.aepd.es/media/informes/2018-0046-investigacionbiomedica.Pdf

[24] Cabe seguir Código Sanitario BOE https://www.boe.es/biblioteca_juridica/codigos/codigo.php?id=084_Codigo_Sanitario&modo=1

[25] Cabe seguir BOE, Código Sanitario Normativa Autonómica, acceso en https://www.boe.es/biblioteca_juridica/codigos/codigo.php?id=212&modo=1&nota=0&tab=2

- Web proyecto PADRIS: http://aquas.gencat.cat/ca/projectes/analitica_dades/
- Web proyecto BIG DATIUS: http://www.bigdatius.com/

IV. ¿CUÁNDO Y DÓNDE SE APLICA LA NORMATIVA DE PROTECCIÓN DE DATOS?

1. ¿Qué son "datos personales", "fichero" y "tratamiento"?

Sin perjuicio del glosario anexo a esta guía, merece la pena detenerse algo más en los conceptos de "datos personales", "fichero" y "tratamiento". No en vano, la interacción de estos conceptos determina que se aplique la normativa de protección de datos.

¿Qué son "datos personales"?

> Datos personales se definen en el RGPD[26] como "toda información sobre una persona física identificada o identificable (el "interesado"); se considerará persona identificable a toda persona cuya identidad pueda determinarse, directa o indirectamente [...], en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, unos datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de la persona.

Cabe alertar de un **equívoco común**, que los datos sean **"personales" no significa** "personales" según socialmente se entiende como equivalente a **"íntimos".** Los datos relativos a personas vinculados a su vida más íntima, en muchos casos serán datos especialmente protegidos (art. 9 RGPD). El Dictamen 4/2007 del Grupo del artículo 29 sobre el concepto de datos personales recuerda que se trata de "Toda información" objetiva o subjetiva y que ni siquiera es necesario que se trate de información cierta."

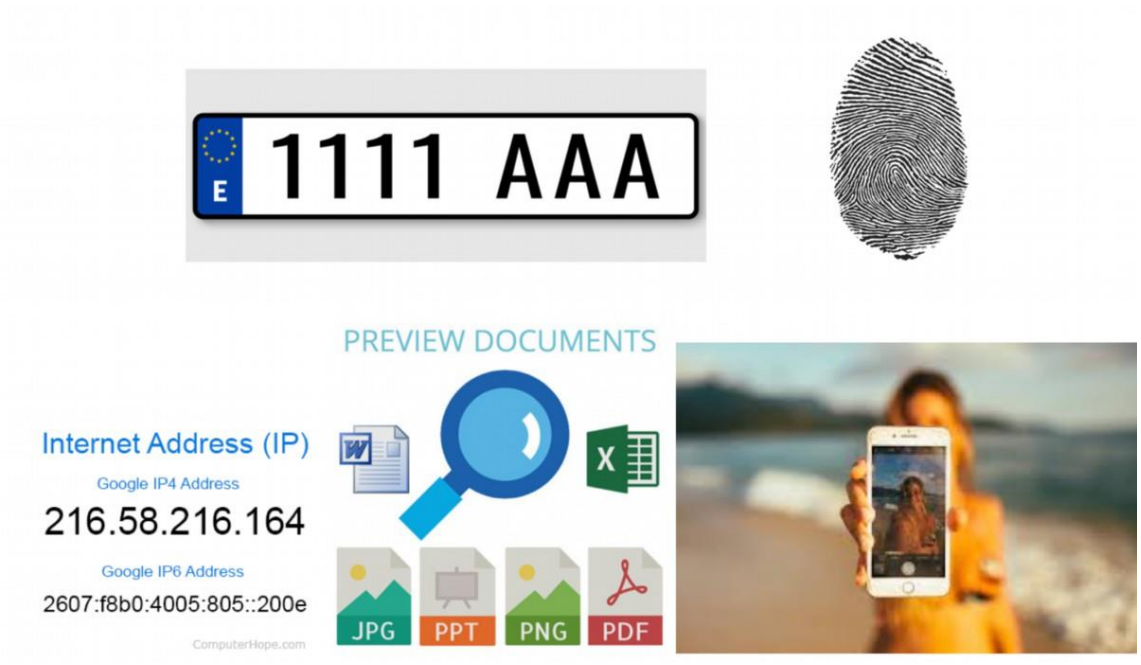
Para que la información se consideren datos personales y se aplique el régimen jurídico **ha de versar sobre una persona física "Identificada o identificable"**. Así pues, aunque no se haya identificado todavía a la persona, basta que sea posible una identificabilidad potencial por singularización, vinculabilidad o inferencia. Determinar la identificabilidad de una información acaba resultando una cuestión esencial, no en vano, como señala el G29 "mientras los datos sean identificables, se aplica la legislación sobre protección de datos".

El **juicio de la identificabilidad** puede ser muy complejo y al final "hay que considerar el conjunto de los medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona, para identificar a dicha persona". El propio RGPD recuerda que para este juicio de identificabilidad "deben tenerse en cuenta todos los factores objetivos, como los costes y el tiempo necesarios para la identificación, teniendo en cuenta tanto la tecnología disponible en el momento del tratamiento como los avances tecnológicos" (Cons. 26). Hay que ir caso por caso de modo contextualizado. Así pues, puede acabar determinándose la identificabilidad en razón de la capacidad, naturaleza,

[26] Al respecto de este concepto de datos personales hay que tener en cuenta el Dictamen 4/2007 del Grupo del artículo 29 sobre el concepto de datos personales.

tamaño, poder económico, empresarial o público del responsable de los datos con relación a que la información pueda llegar a ser relativa a personas concretas. Esto es, que una información sea dato personal o no depende sólo de dicha información, sino del sujeto que la trata y en qué contextos.

Por ejemplo, se ha considerado dato personal la dirección de correo electrónico (Informe de 1999, SAN, Sección 1ª, de 22 de febrero de 2006, rec. 911/2003). Los datos relativos al ejercicio de una profesión (SAN, Sección 1ª, de 11 de febrero de 2004, rec. 119/2002); el Documento Nacional de Identidad (SAN, Sección 1ª, de 27 de octubre de 2004); el número de matrícula de vehículo ha llevado a respuestas contradictorias, no siendo en un dato personal para la SAN 5832 de 26/09/2013. Sí que lo es el número de historia clínica que pueda asociarse con la identidad del paciente (Informe 0283/2008), también el número de teléfono móvil cuando pueda vincularse con el titular de la línea o un número de teléfono (Informe 0575/2008, SAN, Sección 1ª, de 26 de enero de 2005 rec. 1258/2002); las fotografías o la imagen de una persona (Informe 0615/2008, STC 14/2003); el número de una finca en su inscripción registral (informe 0034/2010); un registro de huellas dactilares (Informe 0082/2010). Especialmente controvertido ha sido el caso del número IP. Así, la STJUE de 19 de octubre de 2016, caso C-582/14 considera dato personal a la dirección IP dinámica registrada por un gestor de un sitio de Internet si éste dispone de medios legales que le permitan identificar al usuario.



Imágenes de ejemplos de datos personales o ficheros.

Relacionado con la identificabilidad, está la cuestión de la anonimización, seudonimización y disociación de datos personales, precisamente para evitar la identificabilidad. Se trata de una cuestión esencial, especialmente para el régimen jurídico de la investigación y la protección de datos. A la misma se dedica un apartado de esta guía más adelante.

Además del concepto dato personal resulta de interés tener en cuenta en el RGPD los conceptos de “Datos genéticos”, “Datos biométricos” o “Datos relativos a la salud" ahí definidos. Como se dirá, se trata de datos especialmente protegidos con un régimen jurídico y garantías especiales.

¿Qué es un fichero?

Otro de los vértices del triángulo es el concepto de “fichero”. No en vano se aplica la normativa cuando se tratan datos para ser incluidos en un fichero.

> Para el RGPD lo es “todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica”.
>
> Como el art 5 y 56 Reglamento antigua LOPD ya regulara en España y ahora el artículo 31 LOPD 3/2018, un conjunto estructurado de datos se viene a entender como un fichero cuando puede reconducirse a la unidad en términos lógicos si los múltiples ficheros o aplicaciones están ordenados a una misma finalidad y encontrarse en un mismo repositorio de información.

En cualquier caso, el elemento esencial es que se trate de **información *estructurada*** y que, por ello, sea factible recuperar los datos personales del afectado. Y hay que estar atentos a que existan sistemas o herramientas de indexación que permitan ordenar y localizar información. Y ha llevado a considerar que son ficheros cuando se permiten por ejemplo búsquedas de texto (un mero documento en un procesador de textos); o un fichero por existir una tabla con distintos nombres y direcciones, la agenda de clientes, un conjunto de currículums ordenados o grabaciones de entrevistas de trabajo, registros de imágenes de acceso a locales, una relación de facturas o historiales médicos bajo algún criterio estructural.

> Se ha considerado fichero a efectos de protección de datos a toda página web desde la famosa STJUE caso Lindqvist, C-101/01 de 6 de noviembre 2003 (también SAN 17 de marzo de 2006). Sin embargo, la STS de 19 de septiembre de 2008 no consideró ficheros los libros bautismales por la difícil búsqueda que implicaba su conformación al estar sólo ordenados por fechas y dispersos territorialmente.

¿Qué es un tratamiento de datos?

El triángulo que viene a determinar la aplicación de la normativa de datos personales **se cierra con el concepto de “tratamiento”.**

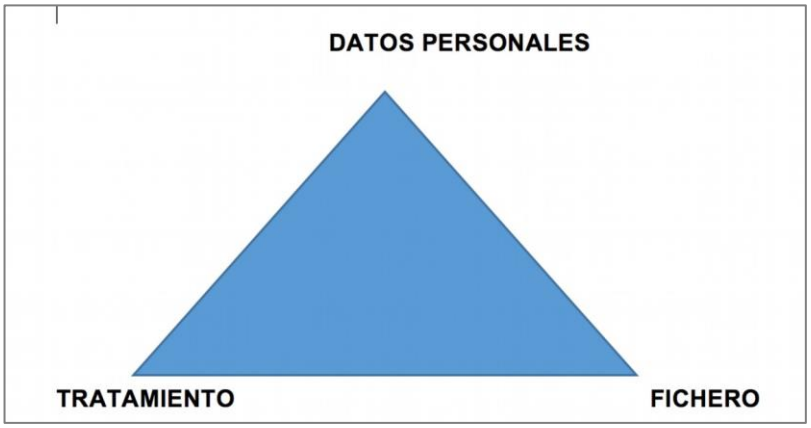
Para el RGPD se trata de "cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción".

Debe ya señalarse que proceder a la anonimización o seudonimización de datos en principio es un tratamiento de datos sujeto a la normativa.

2. ¿Cuándo se aplica el régimen de protección de datos? El triángulo conformado por los vértices de "datos personales", "fichero" y "tratamiento" queda sometido a la normativa de protección de datos

En buena medida, todo lo que quede dentro del triángulo conformado por los vértices de "datos personales", "fichero" y "tratamiento" queda sometido a la normativa de protección de datos.

Así, el Reglamento Europeo de protección de datos (RGPD) en razón de su artículo 2 "se aplica al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero."



Aplicabilidad del régimen de protección de datos cuando hay tratamiento de datos personales estructurados en ficheros.

3. ¿Cuándo no se aplica la normativa de protección de datos?

Hay diferentes supuestos en los que no se aplica la normativa de protección de datos. Ocupará una atención especial y un apartado específico en esta guía el caso de los datos anonimizados[27]. En tanto en cuanto así lo estén completamente, no son datos personales y, en consecuencia, no se aplica la normativa de protección de datos. Basta adelantar que es muy difícil la completa anonimización y, como se ha adelantado, que el mero hecho de anonimizar datos personales es un tratamiento de datos sujeto a la normativa de modo particular. También hay que señalar que el llamado big data o los datos generados por el IOT en muchas ocasiones incluye datos desvinculados de personas, además de desestructurados.

Además de lo anterior, hay que subrayar que la normativa se aplica a los datos relativos a **personas físicas**. Ello lleva, en primer término, a recordar el RGPD "**no regula el tratamiento de datos personales relativos a personas jurídicas** y en particular a empresas constituidas como personas jurídicas (Cons. 14). Así pues, la información sobre empresas, asociaciones, Administraciones, etc. por ejemplo, respecto de su solvencia, localización, información corporativa, económica, etc. no queda afectada por la normativa de protección de datos. Esta exclusión se da, claro está, siempre que dicha información no incluya datos de personas físicas.[28]

En cierto modo **no** se aplican las exigencias de protección de datos respecto del "tratamiento de los datos relativos a los **empresarios individuales y a los profesionales liberales**, cuando se refieran a ellos únicamente en dicha condición y no se traten para entablar una relación con los mismos como personas físicas." (LO 3/2018 en su artículo 19. 2º)

En segundo término, el derecho a la protección de datos lo es respecto de las personas físicas que estén vivas. Así, el RGPD afirma que "**no se aplica a la protección de datos personales de personas fallecidas**" (Cons. 27)[29].

[27] Ver apartado "Especial atención a la anonimización y seudoanonimización…"

[28] Debe llamarse la atención de la exclusión del régimen de protección de datos a la información relativa a las personas jurídicas no implica que no haya un régimen jurídico que proteja, por ejemplo, el derecho al honor de las personas jurídico privadas, o el prestigio de las públicas, así como la importante protección normativa conferida al secreto vinculado a empresas o instituciones, e incluso garantías como la inviolabilidad del domicilio o secreto de comunicaciones.

[29] En todo caso, la LO 3/2018 aunque excluye del ámbito de aplicación de la ley el tratamiento de datos de fallecidos (art. 2.3º d), su art. 3 permite que los herederos puedan solicitar el acceso, rectificación o supresión de los datos, en su caso sujetándose a las instrucciones del fallecido al respecto. Asimismo, la LO 3/2018 incluye como derecho digital un "derecho al testamento digital".

Ello sin perjuicio de la regulación sobre fallecidos en la LO 3/2018[30].

El RGPD **no** es aplicable si un tratamiento es "efectuado por una persona física en el ejercicio de actividades **exclusivamente personales o domésticas**" (art. 2.2.c) RGPD).[31]

Aunque pueda resultar algo confuso, hay que advertir que el hecho de que no se aplique la normativa de protección de datos y en particular el RGPD y la LO 3/2018, no quiere decir que no se aplique otras normativas de ámbitos afines, como pueda ser el derecho al honor, intimidad, propia imagen, la protección de secretos, etc. ya se trate en el ámbito civil, penal, laboral. (por ejemplo: cometer un delito o intromisión por difundir "domésticamente" fotos íntimas de un amigo). En el caso de los datos no personales, sin perjuicio de otras normas, existe incluso el reciente Reglamento (UE) 2018/1807.

[30] Tras excluir del ámbito de aplicación de la ley el tratamiento de datos de fallecidos (art. 2.3º d) art. 3 permite que los herederos puedan solicitar el acceso, rectificación o supresión de los datos, en su caso sujetándose a las instrucciones del fallecido al respecto. Asimismo, la LO 3/2018 incluye como derecho digital un "derecho al testamento digital".

[31] Es especialmente importante tener en cuenta que el RGPD no es aplicable si un tratamiento es "efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas" (art. 2.2.c) RGPD). Se considera en la exclusión los repertorios de direcciones o actividad en redes sociales en estas actividades, eso sí, "sin conexión alguna con una actividad profesional o comercial" (Cons. 18). La previa legislación española (art. 4 a) Reglamento antigua LOPD) concretaba que "solo se considerarán relacionados con actividades personales o domésticas los tratamientos relativos a las actividades que se inscriben en el marco de la vida privada o familiar de los particulares". La sentencia de la Audiencia Nacional de 15 de junio de 2016 señala que "Será personal cuando los datos tratados afecten a la esfera más íntima de la persona, a sus relaciones familiares y de amistad y que la finalidad del tratamiento no sea otra que surtir efectos en esos ámbitos". Baste adelantar que el tratamiento en el ámbito laboral o empresarial, aún realizado en el hogar, no gozaría de esta exclusión. Obviamente hay zonas grises respecto de actividades en internet o redes sociales. Así, el G29 al respecto considera ejemplos que estarían excluidos de la protección de datos, como vender regalos de cumpleaños en una plataforma de e-comercio, tener un blog sobre arreglos florales comentando la propia experiencia laboral, participar en una campaña civil vinculada al ámbito de las flores, compartir datos de interesados en estas aficiones o, incluso, usar sistemas de e-comercio y e-pago para comprar suministros de una afición. Ahora bien, sí quedarían sujetos al RGPD quienes "proporcionen los medios para tratar datos personales relacionados con tales actividades personales o domésticas." (Cons. 18).

Sin perjuicio de lo anterior, es importante tener en cuenta que no nos exime en ningún caso del cumplimiento de nuestras obligaciones de protección de datos[32]:

1. El hecho de que los datos objeto de tratamiento sean públicas u obtenidas de fuentes públicas.
2. El hecho de que los datos se tratan sólo para fines de gestión interna.
3. Que el soporte que contenga o con el que se tratan las bases de datos no sea un software tales como Access, Excel, File Maker etc.
4. Que los datos se encuentran en soportes no automatizados.

4. ¿Dónde se aplica la normativa general de protección de datos?

Por cuanto al importante ámbito de aplicación territorial, el artículo 3. 1º RGPD fija el criterio principal básico de aplicación: que sea un tratamiento de datos "en el contexto de las actividades de un establecimiento del responsable o del encargado en la Unión, independientemente de que el tratamiento tenga lugar en la Unión o no."

Explicado de una manera más simple, se aplica la normativa europea cuando la decisión efectiva de tratar datos personales, o si el tratamiento efectivo de los datos para otro se hace en territorio europeo.

[32] Universidad de Valencia, Protocol d'actuació en matèria de protecció de dades.

https://www.uv.es/fatwireed/userfiles/file/protocoloactuacionprotecciondatos.doc

Resulta especialmente innovador el RGPD cuando extiende el ámbito territorial de aplicación en razón de que el interesado esté en la UE. Así sucede en primer lugar, respecto de: "a) la oferta de bienes o servicios […] independientemente de si a éstos se les requiere su pago" vayan dirigidos a la UE.

> Para "determinarse si es evidente que el responsable o el encargado proyecta ofrecer servicios a interesados en uno o varios de los Estados miembros de la Unión […] la mera accesibilidad del sitio web del responsable o encargado o de un intermediario en la Unión, de una dirección de correo electrónico u otros datos de contacto, o el uso de una lengua generalmente utilizada en el tercer país donde resida el responsable del tratamiento, no basta para determinar dicha intención, hay factores, como el uso de una lengua o una moneda utilizada generalmente en uno o varios Estados miembros con la posibilidad de encargar bienes y servicios en esa otra lengua, o la mención de clientes o usuarios que residen en la Unión, que pueden revelar que el responsable del tratamiento proyecta ofrecer bienes o servicios a interesados en la Unión." (Cons. 23).

En segundo lugar, también **se aplica el RGPD fuera de la UE cuando la actividad de tratamiento sea dirigida al "control de su comportamiento"** (letra b). Y "Para determinar si se puede considerar que una actividad de tratamiento controla el comportamiento de los interesados, debe evaluarse si las personas físicas son objeto de un seguimiento en internet, inclusive el potencial uso posterior de técnicas de tratamiento de datos personales que consistan en la elaboración de un perfil de una persona física con el fin, en particular, de adoptar decisiones sobre él o de analizar o predecir sus preferencias personales, comportamientos y actitudes." (Cons. 24). Sin duda, este criterio tiene un enorme potencial ante el imparable crecimiento de los tratamientos masivos y las decisiones automatizadas.

Pues bien, en estos casos de aplicación extraterritorial, se da un deber de designar expresamente y por escrito un representante en la UE que actúe en nombre del responsable o encargado respecto a las obligaciones que les incumben. En cualquier caso, esta designación no afecta a la responsabilidad del responsable o del encargado, si bien, el representante designado debe estar sujeto a medidas coercitivas en caso de incumplimiento por parte del responsable o del encargado». (Cons. 80).

V. ¿QUÉ TIPOS DE DATOS PERSONALES HAY QUE DISTINGUIR?

En el apartado anterior se vio ¿qué son "datos personales"? Interesa ahora distinguir dentro de los distintos tipos de datos personales por cuanto ello puede conllevar diversas obligaciones y régimen jurídico.

1. Datos personales ordinarios, de carácter identificativo y de características personales.

Dentro de los datos que no implican una especial protección, que podemos denominar ordinarios, puede ser de interés los de carácter identificativo, que pueden ser los que siguen[33]

- Dirección
- IP o identificador
- N. SS /Mutualidad
- Firma
- Marcas Físicas
- Tarjeta Sanitaria
- Firma electrónica
- NIF/DNI
- Teléfono
- Imagen/Voz
- Nombre y apellidos
- Otros (Indique cuáles)
- También es conveniente determinar si se manejan datos de Características personales:
- Circunstancias sociales
- Información comercial
- Detalles del empleo
- Información de scoring o perfilado
- Académicos y profesionales
- Económico, financiera y de seguros

Respecto de estos datos, en principio, el régimen jurídico es el ordinario y general.

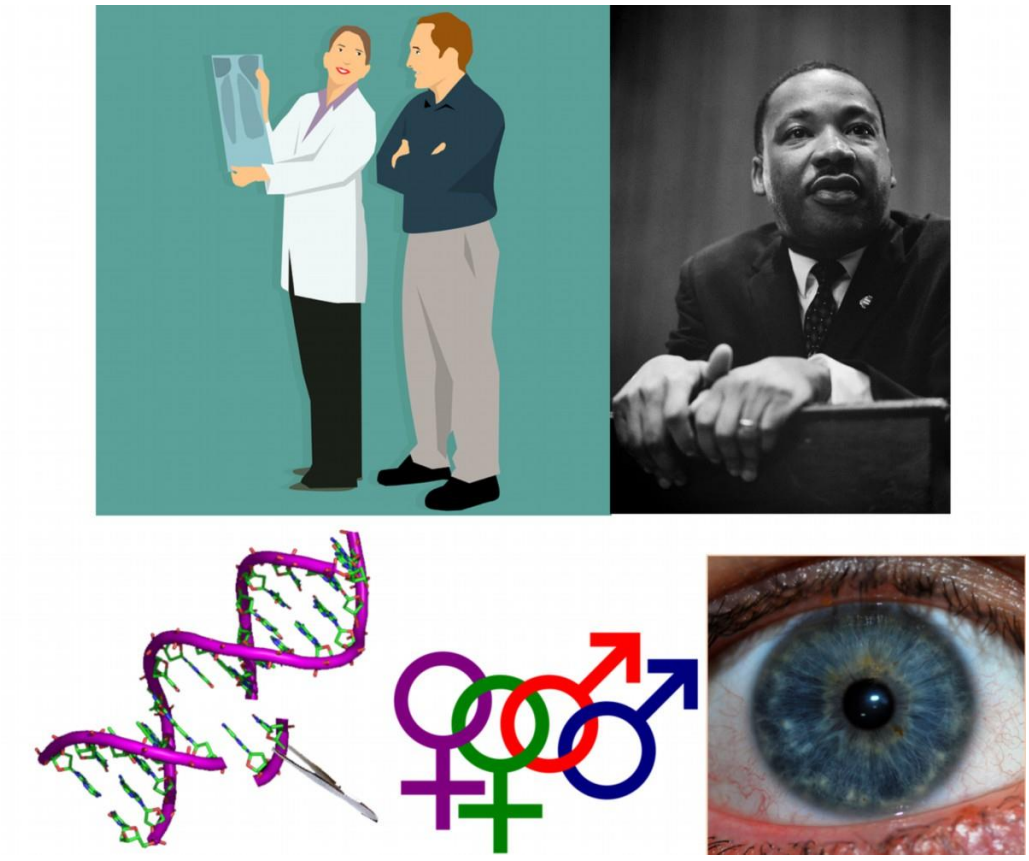
[33] Se siguen, por ejemplo, la tipología del Anexo del mencionado Reglamento del registro de actividades de tratamiento de la UPV 2019.

2. Datos especialmente protegidos o sensibles

La normativa establece un régimen de particular protección respecto de unos datos, por lo que hay que estar especialmente alerta respecto del tratamiento de los mismos.

Así, según el artículo 9 RGPD cabe tener en cuenta datos:

- Afiliación sindical
- Datos biométricos
- Datos relativos a la vida sexual
- Convicciones religiosas o filosóficas
- Datos genéticos
- Datos sobre orientación sexual
- Ideología u opiniones políticas
- Datos relativos a la salud
- Origen Racial o étnico



Ejemplos de datos especialmente sensibles o protegidos

El artículo 4 RGPD define algunos de estos datos especialmente protegidos.

13) «datos genéticos»: datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona;

14) «datos biométricos»: datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos;

15) «datos relativos a la salud»: datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud;

3. Datos estructurados, desestructurados y los crecientes y los muy variados datos relacionados con la salud y utilizados en la investigación

El Consejo de Europa ha recordado el paso desde el término “datos de salud” al más general de "datos relacionados con la salud”. Así, el ámbito de su Recomendación sobre la protección de datos relacionados con la salud, de 27 de marzo 2019[34] es relativa al “al procesamiento de datos personales relacionados con la salud en los sectores público y privado mediante herramientas digitales” (nº 2.1). También el RGPD ha efectuado una “considerable ampliación”[35]; el concepto datos de salud tiene un claro carácter inclusivo en su Considerando 35 RGPD: “Entre los datos personales relativos a la salud se deben incluir todos los datos relativos al estado de salud del interesado que dan información

[34] CONSEJO DE EUROPA, Recomendación CM / Rec (2019) 2 del Comité de Ministros a los Estados miembros sobre la protección de datos relacionados con la salud, de 27 de marzo 2019

Disponible en
https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=090000168093b26e

[35] DÍAZ GARCÍA, Elena, “La entrada en vigor del Reglamento Europeo de Protección de Datos como obstáculo a la investigación”, en *DS : Derecho y salud*, Vol. 28, nº. Extra 1, 2018 (Ejemplar dedicado a: XXVII Congreso: Constitución y Convenio de Oviedo: aniversario de derechos), pp. 231-238, cita p. 234.

sobre su estado de salud física o mental pasado, presente o futuro". Y así debe interpretarse el artículo 4. 15º RGPD que los define[36].

Lo mismo que sucede con el crecimiento de las variadas fuentes de procedencia y las magnitudes de los datos. Ello genera a modo de fuerzas jurídicas en principio contrarias. De un lado, conlleva que son cada vez más también los datos especialmente protegidos del artículo 9 RGPD y sometidos a las especiales garantías del RGPD, lo que puede tener especial incidencia en los requisitos para la legitimación para su uso y, sobre todo, en las garantías y medidas para hacerlo. Ahora bien, antes de someter en bloque todos los datos a un régimen especialmente protegido, es importante segmentar y diferenciar los datos pues ello deberá llevar a soluciones también segmentadas y diferenciadas jurídicamente. Sin embargo, del otro lado, bien es cierto que este creciente conjunto de datos relacionados con la salud, al tiempo que se sujeta al régimen más estricto de los datos especialmente protegidos si se usan para la investigación quedará bajo la tendencia ciertamente contraria de una flexibilización y un régimen más favorable.

Las nuevas fuentes de producción de datos de salud van generando cada vez más datos no estructurados. En este sentido, cabe recordar que los datos pueden ser estructurados, semi-estructurados o no estructurados[37], que son la mayor cantidad.

Los datos cada vez más crecientes y vinculados con el big data, son los no estructurados. Se trata de datos que no tienen modelo u organización[38]. Pueden ser los datos generados por el uso de redes, aplicaciones, sensores, sistemas máquina a máquina o grandes transacciones de gestión de atención y facturación, biometría, etc. Recuerdan Bezhold y Alfonso que los datos y fuentes no estructuradas son muchas más y más variadas[39]. Así, texto libre de las historias clínicas electrónicas, evolutivos o los informes, información enorme cantidad de información en general no estructurada que genera la actividad asistencial. Las imágenes médicas, tanto de pruebas complementarias (radiología,

---

[36] 15) «datos relativos a la salud»: datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud".

[37] ORTEGA GIMÉNEZ, Alfonso, "Implicaciones jurídicas de la internalización de la tecnología del Big Data y Derecho Internacional Privado", en *Revista de derecho y genoma humano: genética, biotecnología y medicina avanzada* nº Extra 1, 2019, pp. 169-204, pp, 176-178.

Igualmente, ALCALDE BEZHOLD, GUILLERMO y ALFONSO FARNÓS, Iciar, "Utilización de tecnología Big Data en investigación clínica", *Revista de derecho y genoma humano: genética, biotecnología y medicina avanzada* nº Extra 1, 2019 , pp. 55-83, en concreto, ver pp. 60 y ss.

[38] ORTEGA GIMÉNEZ, Alfonso, "Implicaciones jurídicas … cit. p. 178, recuerda que SOARES realiza una clasificación de estas fuentes (SOARES, S., "Not Your Type? Big Data Matchmaker On Five Data Types You Need to Explore Today", Big Data Governance. An Emerging Imperative, Ed. MC Press, Boise (Idaho), 2012, pp. 7-8. Disponible en: https://www.dataversity.net/not-your-type-big-data-matchmaker-on-five-data-types-you-need-to-explore-today/

[39] ALCALDE BEZHOLD, Guillermo y ALFONSO FARNÓS, Iciar, "Utilización de tecnología Big Data … cit. pp. 60-61.

ecografía, medicina nuclear, resonancias, electrocardiografía, retinografías, etc.), como fotografías que se adjuntan a la historia clínica. También se incluyen en este apartado las grabaciones en video de procedimientos, incluso la información contenida en las publicaciones científicas. Asimismo, como se ha insistido, hay fuentes alternativas, provenientes de aplicaciones móviles médicas o relacionadas con la salud, generadas por diferentes dispositivos portátiles, además redes sociales generales o específicas de salud y los metadatos de todos los dispositivos.

La estructuración de los datos puede tener fuerte incidencia jurídica. Como es sabido, son elementos muy importantes para aplicar el régimen de protección de datos la estructuración de los mismos en ficheros o sistemas datos, así como, especialmente, la posibilidad de identificabilidad de los datos con relación a una persona y, por tanto, su cualidad de personales. Según cada caso, si no llegan a considerarse datos personales y no superan un juicio de identificabilidad (Cons. 26 RGPD) los datos no estructurados podrán escapar más fácilmente al régimen de protección de datos. Si no son datos identificables, vinculables a una persona, no son datos personales y, por tanto, no se aplicaría este régimen jurídico. Especialmente en los supuestos en los que se necesiten esfuerzos desproporcionados o altas capacidades para que los datos no estructurados puedan ser identificables y, por tanto, personales. Este análisis obviamente depende de la naturaleza y cualidad de los datos de los que se trate, pero lo cierto es que se tiene esencialmente al responsable que trata datos, esto es, se efectúa teniendo en cuenta las capacidades objetivas del responsable del tratamiento. Así lo ha recordado la propia AEPD respecto del big data[40].

Asimismo, la no estructuración puede condicionar mucho los potenciales usos que pueden tener los datos. También la estructuración determinará la necesidad de efectuar algunos tratamientos previos para que puedan ser útiles para la investigación y habrá de pensarse en la legitimación de dichos tratamientos previos. Igualmente, la mayor o menor estructuración será relevante técnicamente para la aplicación de medidas de seguridad y especialmente la posibilidad o necesidad de seudonimización. Respecto de los datos no estructurados sobre los que muchas veces ni se sospechan posibles finalidades resultan dificultades para el cumplimiento de la transparencia o la legitimación de ulteriores comunicaciones.

4. Otros tipos de datos –o tratamientos- con un régimen o garantías especiales, como el necesario estudio de impacto

Aunque no están bajo el régimen particular del artículo 9 RGPD de datos especialmente protegidos, también hay que tener especiales cautelas respecto de:

- datos de menores, especialmente si se trata de menores de 14 años.

[40] AEPD - ISMS Forum (eds.); Carlos Alberto Sáiz (coord.). (2017). *Código de buenas prácticas en protección de datos para proyectos de Big Data*, mayo, AEPD e ISMS Forum, Madrid, pp. 9 y ss. También, STJUE 19 de octubre de 2016, Asunto C-582/14, Patrick Breyer v. Alemania.

- datos de sujetos vulnerables o en riesgo de exclusión social, incluyendo datos de mayores con algún grado de discapacidad, discapacitados, personas que acceden a servicios sociales y víctimas de violencia de género, así como sus descendientes y personas que estén bajo su guardia y custodia
- los datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10 RGPD. Asimismo, y por tradición normativa, los relativos a sanciones de infracciones administrativas.
- Video vigilancia de espacios públicos.

Como se señalará[41], bajo el principio de responsabilidad proactiva se incluye también la obligación de realizar un estudio de impacto de protección de datos en algunos supuestos (art. 35 RGPD).[42] Sobre esta base y para España, la AEPD en 2019 ha concretado las Listas de tipos de tratamientos de datos que requieren EIPD (art 35.4) [43]. Señala que será **necesario** realizar un estudio de impacto en la mayoría de los casos en los que dicho **tratamiento cumpla con dos o más criterios de la lista** expuesta a continuación. Añade que cuantos más criterios reúna el tratamiento en cuestión, mayor será el riesgo que entrañe dicho tratamiento y mayor será la certeza de la necesidad de realizar una EIPD. Del listado no exhaustivo de once tratamientos de mayor riesgo que se recogen en el documento, en el ámbito que aquí interesa, debe haber especial sensibilidad y alerta cuando se traten datos:

- que impliquen perfilado o valoración de trabajo, personalidad y comportamiento
- datos y metadatos a través de redes, aplicaciones o en zonas de acceso público
- procesamiento de identificadores únicos que permitan la identificación de usuarios de servicios de la sociedad de la información como pueden ser los servicios web, TV interactiva, aplicaciones móviles, etc.

[41] Apartado "¿Qué obligaciones hay que cumplir si se tratan datos y qué medidas hay que adoptar?".

[42] La norma europea impone esta especial garantía respecto de ámbitos que son bien afines al ecosistema inteligencia artificial-big data. Así:

- Evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar
- Tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9, apartado 1 (datos especialmente protegidos), o de los datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10,
- La observación sistemática a gran escala de una zona de acceso público.

[43] Pág. 3.

- datos especialmente protegidos artículo 9.1 del RGPD y datos relativos a condenas o infracciones penales, 10 del RGPD. Datos biométricos, datos genéticos.
- datos de situación financiera o de solvencia patrimonial
- sujetos vulnerables o en riesgo de exclusión social, incluyendo datos de menores de 14 años, mayores con algún grado de discapacidad, discapacitados, personas que acceden a servicios sociales y víctimas de violencia de género.

Imágenes de datos o tratamientos con garantías especiales.

Por cuanto a los tipos de tratamientos, propios e incluso **naturales del ecosistema del big data y la inteligencia artificial**, se incluye la garantía del estudio de impacto respecto de:

- toma de decisiones automatizadas
- perfilados de comportamiento.
- uso de datos a gran escala
- asociación, combinación o enlace de registros de bases de datos para varias finalidades.
- utilización de nuevas tecnologías o un uso innovador de tecnologías consolidadas, incluyendo la utilización de tecnologías a una nueva escala, con un nuevo objetivo o combinadas con otras

Sobre la base de lo anterior, en el marco de una gobernanza de datos dentro de la organización al proponer un tratamiento o fichero de datos habrá que tener clara la tipología de los datos, así como los posibles afectados o interesados (personas físicas de quienes se tratan datos).

VI. QUIÉN ES QUIÉN DESDE LA PROTECCIÓN DE DATOS Y SUS OBLIGACIONES. LA GOBERNANZA DE LOS DATOS EN LAS ORGANIZACIONES

1. Gobernanza y procesos internos en las organizaciones

Se habla de **«Data Governance" o la "gobernanza de los datos"** al conjunto de acciones, gestión, procesos, funciones, políticas, normas y mediciones que ha de haber en una organización que trata datos. Implica una estrategia integral con una orgánica y responsabilidad, procedimientos y plan de gestión global todos los datos de la organización. Se busca así que sea eficiente, eficaz y garantice el cumplimiento normativo.

Cada organización tiene y determina su organización y procesos y, obviamente, adopta su gobernanza de datos. El esquema habitual de gobernanza de datos dentro de la organización pasa por procedimientos internos, normas y protocolos que se establezcan en materia de protección de datos[44]. Y hay que estar por lo que ahí se establezca.

No obstante, **la normativa de protección de datos fija unos sujetos con deberes y responsabilidades específicos** que hay que tener en cuenta. A este respecto, cabe remitir al posterior apartado relativo a "Procesos internos de autorización de tratamientos de datos y registro de actividades", en el marco del apartado dedicado a las obligaciones por tratar datos y qué medidas hay que adoptar, ahí se expondrá y concretará el nuevo modelo del RGPD que impone a cumplir de modo proactivo toda una serie de obligaciones a quien trate datos personales.

En todo caso, y como **pauta general** y especialmente **a fin de cumplir la obligación del registro de actividades de tratamiento**, los miembros del Data Space respecto de la organización de la que forman parte, habrán de **comunicar la necesidad** y las características básicas del tratamiento de datos que se quiere llevar a cabo y qué tipo de datos van a manejar. Así, suelen formalizarse procedimientos para comunicar quién será la unidad que quiere tratar datos, si va a haber varios responsables que de datos dentro y fuera de la organización, la finalidad o finalidades que se persiguen, el tipo de datos, las estructura del conjunto de datos, tipología de los interesados o afectados, el origen de los datos, si está previsto que haya encargados que vayan a manejar datos en razón de contrato o instrumento jurídico, si está previsto comunicar los datos a otros (terceros). Cada Universidad, instituto, organización establece los procedimientos internos como si se requieren informes técnicos o jurídicos cuando se da la comunicación de los elementos anteriores.

También es habitual que se aplique este esquema o haya un procedimiento por cuanto lo que vaya a realizarse es un diseño de sistemas, software, aplicaciones dirigido al tratamiento de datos personales.

[44] Ver al apartado anterior "Normativas y protocolos internos".

Sobre esta información el DPD –si lo hay- en la organización o persona similar debe **evaluar riesgos y planificar la mitigación de impactos**, sobre esta base se proponen las **medidas de seguridad** aplicables, cómo garantizar el principio de **transparencia e información o cómo satisfacer los derechos** de los interesados y las relaciones con terceros.

Es habitual que una unidad en la organización –bajo la autoridad y asesoría del DPD- asuma la atribución de autorizar los tratamientos de datos. Cada orgánica determina figuras responsables internas del tratamiento.

Así, por ejemplo, para la Universidad Politécnica, cabe seguir los artículos 3 y 13 Reglamento del registro de actividades de tratamiento de la Universitat Politècnica de València.

O los diferentes roles que establece la UNED: Responsabilidades: Responsable de Seguridad de los tratamientos; Gestor de Tratamiento; Comité de Seguridad de la Información (*Código de Conducta* UNED, 2.11).

La **orgánica interna debe conectarse con el organigrama de la organización** (por ejemplo, Secretaría General de la Universidad, Gerencia, etc.).

Además de un **esquema de autorización interna de tratamientos**, el reparto de papeles lleva a **distribuir funciones** concretas relativas al cumplimiento de medidas de seguridad, responsabilidad ante ejercicio de derecho de acceso, comunicación con autoridades, supervisión de contratos y documentos de encargados de tratamiento, etc.

Así, procede seguir quién es quién desde la protección de datos. A la hora de estructurar la fuente, el flujo de datos, la investigación a proceder, los tratamientos previstos, habrá que determinar si se trata de múltiples responsables de datos a través de la entidad de investigación o de un responsable (por ejemplo, la fuente de los datos, que en su caso contrata a un encargado para que maneje los datos para sus finalidades). De igual modo es muy posible que lo que se prevea sea una comunicación de datos entre los componentes de la investigación en el seno de la entidad de investigación o con terceros. Cada caso tiene un régimen jurídico diferente.

Un modelo de gobernanza de datos obliga a tener una estrategia y visión de quién es quién en cada tratamiento de datos. Es muy importante desde el inicio diseñar las estrategias en la captación o fuentes de datos, así como el flujo de datos entre responsables, encargados o cesiones de datos a terceros.

Como se ha adelantado la normativa de protección de datos se aplica cuando se da un tratamiento de datos en el contexto de actividades de un establecimiento de un responsable o de un encargado en la UE.

2. ¿Quién o quiénes son los "responsables" de un tratamiento de datos?

El "**responsable**" es "la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento". Una persona jurídica muy habitualmente será un responsable, por ejemplo, una Administración, una empresa o una asociación. El elemento básico es la toma de decisiones sobre la creación y finalidades del tratamiento de datos. Quién materialmente adopta estas decisiones es el responsable del tratamiento.

ITI es una asociación con personalidad jurídica que puede adoptar la decisión de un tratamiento y disponer los medios y fines.

La cuestión se torna ciertamente compleja en ecosistemas como el Data Space, y en general en i-Spaces. Se trata de una variedad de estructuras técnicas y organizativas de integración o agregación de datos para la investigación (en su caso también de infraestructura, recursos, Hardware, Software, herramientas, algoritmos y servicios). Cabe tener en cuenta asimismo las variedades de data hubs, data lakes o almacenes de datos. Así pues, en estas estructuras técnicas y organizativas puede ser muy habitual una **pluralidad de responsables** y habría que atender en cada caso al tratamiento concreto que se trate y el ámbito y alcance decisional. (Y estas fórmulas hay que analizarlas también conjuntamente con la figura de "encargado" que se analiza a continuación, puesto que la entidad de investigación como ITI o las entidades que integran un data space bien pueden tratar datos no por su cuenta propia, sino para prestar servicios o realizar investigaciones concretas por cuenta de otro sujeto, por ejemplo).

Las decisiones bien pueden ser conjuntas bajo distintas fórmulas de colaboración, acuerdos, consorcio, convenio, contrato, etc. Resulta especialmente de interés determinar desde inicio quiénes participan y en calidad de qué.

El tratamiento de datos bien puede generarse por las necesidades en el marco de proyectos de investigación subvencionados, en estos supuestos hay que tener en cuenta la posibilidad de distintas entidades en el ámbito de la investigación y las posibles particularidades en la gobernanza y determinación de papeles tanto en el proyecto solicitado como en el marco jurídico concreto de la subvención.

La nueva LOPD (artículo 29), concreta que para determinar las responsabilidades debe atenderse a las actividades que efectivamente desarrolla cada uno de los responsables del tratamiento.

Así pues y, en cualquier caso, sin perjuicio de lo que puedan decir los acuerdos al respecto, la determinación de quién o quiénes son los responsables depende de la realidad material de la decisión de hacer el tratamiento, y la puesta de medios.

Así, desde el inicio habrá que **determinar** todos los posibles sujetos participantes en el tratamiento en calidad de **responsables**.

Por ejemplo, determinar[45] si el tratamiento ha sido realizado conjuntamente con:

- Otra Universidad
- Instituto mixto de investigación
- Una empresa privada
- Una asociación (estudiantes, científica etc.)
- Una fundación
- Otro equipo de investigación
- Otra administración
- Otra entidad privada no empresarial

No confundir: Cabe recordar que **quienes actúen bajo autoridad directa del responsable o del encargado**, por ejemplo, los trabajadores del instituto, empresa, Administración o asociación se consideran en el ámbito de tal sujeto obligado y no hay que confundirlos con el "encargado" del tratamiento y, obviamente, tampoco son terceros.

[45] Se sigue, por ejemplo, anexo, Reglamento del registro de actividades de tratamiento de la Universitat Politècnica de València.

3. ¿Quién es el "encargado" y cuáles son las obligaciones y requisitos en la contratación?

Por su parte, el **"encargado del tratamiento o encargado"** es "la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento", si bien, no están bajo la autoridad directa de éste, sino que están **unidos a través de un marco contractual u otra fórmula jurídica**.

Ejemplos de encargados: La **subcontratación de servicios** –por ejemplo, de mantenimiento informático- es un claro ejemplo de encargado que trata datos por cuenta del responsable, o las empresas marketing, de consultoría de protección de datos, de instalaciones de cámaras de videovigilancia, administradores de fincas, agentes de seguros, procuradores, abogados, etc. Cabe tener en cuenta que una empresa de un grupo de empresas puede en su caso actuar como encargado. En ocasiones puede llamar la atención que un responsable de tratamiento sea un mero usuario de servicios de la nube y el encargado del tratamiento sería en principio el prestador de servicios de la nube por cuenta del cliente.

En el **ámbito de la Universidad, la figura de encargados** en el tratamiento de datos es habitual respecto de las siguientes finalidades[46]:

- Mantenimiento y soporte de aplicaciones informáticas (bolsa empleo, participación de estudiantes).
- Mantenimiento de la enseñanza virtual.
- Mantenimiento de la plataforma de la gestión académica del alumnado.
- Impresión de los títulos universitarios.
- Guarda y custodia de la documentación del Archivo General.
- Servicio de mensajería.
- Servicio de fotografía profesional.
- Mantenimiento de los relojes de control horario.
- Soporte de la gestión económica y de Recursos Humanos.
- Distribución y ventas de la Editorial.

El marco jurídico será muy importante para determinar los papeles que se ocupan y, sobre todo, la normativa obliga a fijar en el marco contractual o jurídico el régimen de deberes y responsabilidades en el marco de la protección de datos entre el responsable y el encargado.

[46] Código de conducta UNED, cit.

Como recuerda la reciente Guía Requisitos para auditorías… Deben quedar claros la identificación y contacto de responsables, corresponsables, representantes del responsable y de los encargados, dpo si lo hay, quedando inscritos en el registro de actividades de tratamiento. Especialmente importante resulta identificar los contratos de encargado.

El artículo 28 del RGPD señala las condiciones en aquellos supuestos en los que un tercero (Encargado de Tratamiento) preste un servicio a miembros de la estructura de investigación o experimentación como el Data Space que conlleve un acceso a datos de carácter personal. Así:

-elegirá únicamente un encargado que ofrezca garantías. Hay responsabilidad por una mala elección. Debe demostrarse que se ha analizado los riesgos de la elección.

-se regirá por un contrato u otro acto jurídico que vincule al encargado respecto del responsable y establezca el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable. La AEPD ha establecido un contrato modelo para el encargado que hay que seguir, con las adecuaciones que incluya la propia organización. Directrices para la elaboración de contratos entre responsables y encargados del tratamiento

-Se trata de garantizar que el encargado tratará los datos personales únicamente siguiendo instrucciones del responsable.

-Límites a la subcontratación a un tercero por el encargado: el encargado del tratamiento no recurrirá a otro encargado sin la autorización previa por escrito, específica o general, del responsable. Si existe, el encargado informará al responsable de cualquier cambio previsto en la incorporación o sustitución de otros encargados. Cuando un encargado del tratamiento recurra a otro encargado se ha de garantizar en todo caso el cumplimiento de las mismas obligaciones de protección de datos. Asimismo, existe el deber de guardar secreto profesional. La fijación y expresión concreta de estos compromisos es especialmente útil.

La **nueva LOPD** incluye algunas novedades o particularidades respecto de los encargados (artículos 28 y 33)[47].

[47] En relación con los encargados de las Administraciones Públicas (como pueda ser una Universidad) artículo 33. 2 dispone si el encargado actúa en su propio nombre y sin que conste que actúa por cuenta de otro, estableciendo relaciones con los afectados aun cuando exista un contrato o acto jurídico con el contenido fijado en el artículo 28.3 del RGPD, será considerado responsable

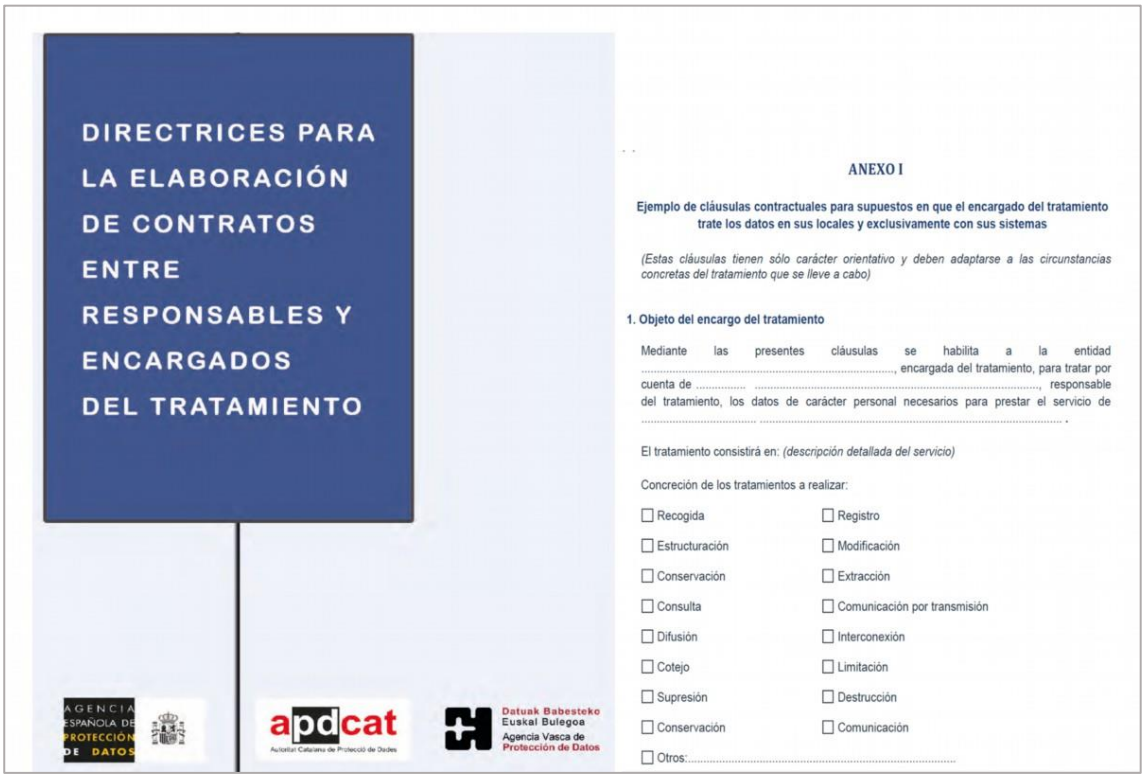
Tendrá asimismo la consideración de responsable del tratamiento quien figurando como encargado utilizase los datos para sus propias finalidades.

Cuando se produce un cambio de encargado el responsable del tratamiento determinará si, cuando finalice la prestación de los servicios del encargado, los datos personales deben ser destruidos, devueltos al responsable o entregados, en su caso, a un nuevo encargado. No obstante, no procederá la destrucción de los datos cuando exista una previsión legal que obligue a su conservación, en cuyo caso deberán ser devueltos al responsable, que garantizará su conservación mientras tal obligación persista.

En el ámbito del sector público podrán atribuirse las competencias propias de un encargado del tratamiento a un determinado órgano de la Administración General del Estado, la Administración de las comunidades autónomas, las Entidades que integran la Administración Local o a los Organismos vinculados o dependientes de las mismas mediante la adopción de una norma reguladora de dichas competencias, que deberá incorporar el contenido exigido por el artículo 28.3 del RGPD.

Según la Disposición transitoria quinta: Los contratos de encargado del tratamiento suscritos con anterioridad al 25 de mayo de 2018 al amparo de lo dispuesto en el artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal mantendrán su vigencia hasta la fecha de vencimiento señalada en los mismos y en caso de haberse pactado de forma indefinida, hasta el 25 de mayo de 2022.

Durante dichos plazos cualquiera de las partes podrá exigir a la otra la modificación del contrato a fin de que el mismo resulte conforme a lo dispuesto en el artículo 28 del Reglamento (UE) 2016/679 y en el Capítulo II del Título V de esta ley orgánica.



Directrices para elaboración de contratos responsable-encargados.

Resulta de especial utilidad seguir las Directrices para la elaboración de contratos entre responsables y encargados del tratamiento de la AEPD y otras autoridades de protección de datos así como su **anexo con modelo de Ejemplo de cláusulas contractuales** para supuestos en que el encargado del tratamiento trate los datos en sus locales y exclusivamente con sus sistemas.

4. Es esencial fijar desde el inicio el marco jurídico de acceso y responsabilidades a datos

Hay que insistir que en el ecosistema del big data y la inteligencia artificial, así como en el ámbito de la investigación, no será en modo alguno extraña la contratación de servicios especializados que impliquen el tratamiento de datos entre los mismos miembros del Data Space (o estructura de investigación) o de empresas terceras. ITI o entidades integradas en la estructura de investigación bien pueden tratar datos para prestar servicios o realizar investigaciones concretas por cuenta de otro sujeto, por ejemplo. En todos los casos, deben seguirse las exigencias y poner al tanto al DPD.

Una mala gestión del marco jurídico de responsabilidades de protección de datos puede condicionar o incluso imposibilitar el desarrollo del servicio o investigación por no permitir el acceso o comunicación de datos.

El Data Space (o estructura de investigación), en su caso universidad, instituto, organización debe tener bien clara en sus fórmulas de contratación y subcontratación si para ello ha de tratar datos personales, qué tratamientos, en calidad de qué. Si es el caso obligatoriamente ha de recoger en el clausulado el régimen específico de facultades y responsabilidades de protección de datos ya como responsable, corresponsable, encargado, etc.

5. ¿Qué es el delegado de protección de datos (DPD)?, obligatorio en el ámbito de la Inteligencia artificial y big data

Bajo el nuevo modelo de responsabilidad proactiva, se incluye una garantía material del cumplimiento normativo. Así, el artículo 38 RGPD regula al delegado de protección de datos (DPD). El mismo puede ser obligatorio (art. 37) o voluntario en las organizaciones que tratan datos personales. El DPD pasa a ser una figura clave para el cumplimiento normativo.

¿Qué hace el DPD? Esencialmente (art. 39) el DPD informa y asesora al responsable o al encargado del tratamiento y a los empleados en materia de protección de datos; supervisa el cumplimiento de la normativa, realiza consultas, coopera y es punto de contacto con las autoridades de protección de datos, notifica las violaciones de seguridad, realiza evaluaciones de impacto y analiza la protección de los datos desde el diseño y por defecto. Asimismo, se encarga de la planificación, y la gestión y la supervisión de las medidas de seguridad aplicable a tratamiento de datos en la organización, supervisa las auditorías correspondientes y la asignación de responsabilidades sobre protección de datos. La nueva LOPD incluye su atribución de intervenir en la resolución de reclamaciones, tanto las recibidas directamente de los interesados como de la AEPD.

¿Cuál es su posición? Para todo ello ha de garantizarse que tenga una posición adecuada en la organización y se garantice que no reciba ninguna instrucción, ni pueda ser sancionado o destituido por desempeño de sus funciones y sólo responda al nivel jerárquico más alto.

¿Es obligatorio? En el ecosistema de la inteligencia artificial, big data etc. es más que posible que la figura sea obligatoria porque casi de modo seguro se da alguno de las condiciones para que sea obligatorio:

- siempre que se trate de organismos públicos, como cualquier ente en el ámbito de una Universidad o institución de investigación pública.
- organizaciones que lleven a cabo una observación habitual y sistemática de interesados a gran escala.
- tratamiento a gran escala de categorías especiales de datos personales (artículo 9) o de datos relativos a condenas e infracciones penales a que se refiere el artículo 10.

VII. UN RÉGIMEN GENERAL MÁS FLEXIBLE Y FAVORABLE PARA LA INVESTIGACIÓN CIENTÍFICA

Cuando se quieren usar datos personales para la investigación, el RGPD excepciona, flexibiliza o relaja algunas de sus exigencias *a cambio* de garantías.

El RPGD es consciente del valor social de la investigación que maneja datos. Así, combinando información procedente de registros, los investigadores pueden obtener nuevos conocimientos de gran valor sobre condiciones médicas y los resultados de las investigaciones pueden ser más sólidos, ya que se basan en una población mayor. Dentro de las ciencias sociales, la investigación basada en registros permite que los investigadores obtengan conocimientos esenciales acerca de la correlación a largo plazo, con otras condiciones de vida, de diversas condiciones sociales, como el desempleo y la educación. Así, estos conocimientos sólidos y de alta calidad que pueden servir de base para la concepción y ejecución de políticas basadas en el conocimiento, mejorar la calidad de vida de numerosas personas y mejorar la eficiencia de los servicios sociales. Y, en general y por ello, al Derecho de la Unión le basta con la seudoanonimización para el tratamiento lícito de los datos.[48].

Como punto de partida de este régimen particular más favorable, hay que concretar **¿qué se considera "investigación"?**

Según el Considerando 159 RGDP, debe interpretarse de modo amplio el concepto de "investigación científica", de modo "que incluya, por ejemplo, el desarrollo tecnológico y la demostración, la investigación fundamental, la investigación aplicada y la investigación financiada por el sector privado. […] Entre los fines de investigación científica también se deben incluir los estudios realizados en interés público en el ámbito de la salud pública."

También cabe señalar que la investigación que goza de las ventajas regulatorias se vincula en el Considerando 33 y en el artículo 89 RGDP a aquella en la "que respeten las normas éticas reconocidas para la investigación científica". El GT29 ha recordado que el término "investigación científica" "no está definido" en el RGPD.[49] No obstante, advierte que "el GT29 considera que la noción no debe ampliarse más allá de su significado común y entiende que «investigación científica» en este contexto se refiere a un proyecto de investigación establecido con arreglo a las correspondientes normas metodológicas y

[48] Díaz García, Elena, "La entrada en vigor del Reglamento Europeo de Protección de Datos como obstáculo a la investigación", en *DS : Derecho y salud,* Vol. 28, Nº. Extra 1, 2018, págs. 231-238, p. 237

[49] GRUPO DE TRABAJO DEL ARTÍCULO 29, *Directrices sobre el consentimiento en el sentido del Reglamento (UE) 2016/679*, adoptadas el 28 de noviembre de 2017, se sigue revisión 10 de abril de 2018, p. 31. Su última revisión en mayo de 2020 *Guidelines 05/2020 on consent under Regulation 2016/679* disponible en https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf

éticas relacionadas con el sector, de conformidad con prácticas adecuadas".[50] En este punto, Alkorta ha advertido que no hay una normatividad homogénea de la investigación, sino más en cada disciplina. Y también siguiendo a esta autora, puede interpretarse que, para gozar de las ventajas regulatorias, la investigación pública o privada debe permitir que se pueda acceder al resultado de la investigación a través de la publicación o de otro medio que garantice "la libre circulación de los conocimientos científicos y tecnológicos" (según el Tratado de Funcionamiento UE al que hace referencia el RGPD). En consecuencia, en modo alguno hay que excluir del régimen más favorable a la investigación del sector privado y sin fondos públicos. No obstante, en estos supuestos puede ser un elemento relevante que la investigación privada bajo el régimen más favorable del RGPD quede vinculada con más o menos elementos de circulación del conocimiento y apertura del mismo. En todo caso, hay que esperar interpretaciones por tribunales o autoridades de protección de datos europeas o nacionales, y especialmente del Comité Europeo (EDPB).

A falta de interpretaciones por tribunales o autoridades de protección de datos europeas o nacionales, puede también interpretarse que, para gozar de las ventajas regulatorias, la investigación pública o privada permita que se pueda acceder al resultado de la investigación a través de la publicación o de otro medio que garantice "la libre circulación de los conocimientos científicos y tecnológicos" (según el tratado al que hace referencia el RGPD) [51].

La regla específica básica se encuentra en el artículo 89 RGPD explicado en buena medida en el Considerando (157)[52]. El mismo viene a señalar que con garantías como la

[50] Ídem.

[51] En este sentido, Alkorta Idiakez Itziar, "Regulación del tratamiento de los datos en proyectos de investigación sanitaria, en especial, en la aplicación de las tecnologías Bigdata", en *Revista de derecho y genoma humano: genética, biotecnología y medicina avanzada* Nº Extra 1, 2019 (Ejemplar dedicado a: Uso de datos clínicos ante nuevos escenarios tecnológicos y científicos. Oportunidades e implicaciones jurídicas), págs. 273-323, p. 298.

[52] "El tratamiento ulterior de datos personales con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos ha de efectuarse cuando el responsable del tratamiento haya evaluado la viabilidad de cumplir esos fines mediante un tratamiento de datos que no permita identificar a los interesados, o que ya no lo permita, siempre que existan las garantías adecuadas (como, por ejemplo, la seudonimización de datos). Los Estados miembros deben establecer garantías adecuadas para el tratamiento de datos personales con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos. Debe autorizarse que los Estados miembros establezcan, bajo condiciones específicas y a reserva de garantías adecuadas para los interesados, especificaciones y excepciones con respecto a los requisitos de información y los derechos de rectificación, de supresión, al olvido, de limitación del tratamiento, a la portabilidad de los datos y de oposición, cuando se traten datos personales con fines de archivo en interés público, fines de

seudoanonimización cada país puede establecer excepciones y flexibilizaciones de las reglas generales para la investigación *como regla general no se considera incompatible usar los datos para la investigación si se cumplen unos requisitos* asimismo se dan facilidades para considerar un uso legítimo de datos, menores obligaciones de transparencia o de garantizar derechos, etc.

El artículo 89. 1º RGPD facilita el uso para la investigación *a cambio* de "garantías adecuadas", esencialmente de "garantizar el respeto del principio de minimización de los datos personales" y para ello se mencionan técnicas de seudonimización "Siempre que esos fines [de la investigación concreta] pueden alcanzarse mediante un tratamiento ulterior que no permita o ya no permita la identificación de los interesados".

Como recuerda la CRUE[53] para el tratamiento de datos personales con fines históricos, científicos o estadísticos se ha de estar a las siguientes reglas:

a. Los datos personales han de limitarse a los estrictamente necesarios y limitados a la finalidad científica concreta que se persigue.

b. Se han de ofrecer las garantías previstas en el artículo 89 RGPD ("seudonimización", cifrado, etc.).

c. Los miembros del grupo de investigación deberán respetar el deber de confidencialidad que establece el artículo 5.1 de la LOPDGDD.

d. La finalización del estudio debe comportar necesariamente la eliminación de los datos personales de las personas interesadas.

Como he tenido ocasión de sostener detenidamente, hay que partir de un principio *pro investigatione* a la hora de interpretar el complejo y no pocas veces oscuro marco jurídico de la protección de datos en la investigación[54]. En esta dirección, la exposición de motivos LO 3/2018 habla de una "interpretación extensiva de las mismas" para el caso de "uso de

investigación científica e histórica o fines estadísticos. Las condiciones y garantías en cuestión pueden conllevar procedimientos específicos para que los interesados ejerzan dichos derechos si resulta adecuado a la luz de los fines perseguidos por el tratamiento específico, junto con las medidas técnicas y organizativas destinadas a minimizar el tratamiento de datos personales atendiendo a los principios de proporcionalidad y necesidad. El tratamiento de datos personales con fines científicos también debe observar otras normas pertinentes, como las relativas a los ensayos clínicos."

[53] Guía de buenas prácticas en materia de Transparencia y Protección de Datos, cit.

[54] COTINO HUESO, L. "El alcance e interactuación del régimen jurídico de los datos personales y big data relacionado con salud y la investigación biomédica", *Revista de derecho y genoma humano: genética, biotecnología y medicina avanzada*, nº 52, 2020.

sus datos sin consentimiento en el ámbito de la investigación biomédica."[55]. La AEPD antes incluso de la ley ya tenía una visión favorable a esta tendencia facilitadora, como se muestra en especial en su Informe 073667/2018[56]. En la materia hay que tener especialmente en cuenta los dictámenes de la Autoridad Catalana de Protección de Datos CNS 15 y 18/2019[57].

Ahora bien, esta inercia y principio interpretativo es en principio contraria a la mayor protección y garantías respecto de los tratamientos de datos especialmente protegidos (art. 9 RGPD), como los relacionados con la salud. Cabe sostener que estas dos inercias contrarias lo que implican es que haya una mayor sujeción al Derecho, posibilidad de control y garantías, especialmente frente a los tratamientos de datos desestructurados y masivos, pero sin que ello necesariamente deba suponer una barrera efectiva a la investigación de interés público. Un marco de flexibilidad contenido y controlado[58].

De hecho, en la actualidad la gran olvidada en España es la regulación del uso de inteligencia artificial y big data no relativos a la investigación biomédica. Se trata de un problema que puede dejar en la alegalidad a muy importantes investigaciones. Considero y he sostenido que ***debe partirse como mínimo de que la investigación no biomédica debe contar con las ventajas de la biomédica por cuanto a la flexibilización de su régimen***. Ello

---

[55] En concreto lo hace respecto de la regulación existente sobre investigación como válida como base legal para el uso de datos, en especial para el ámbito biomédico"

Así, en la Exposición de motivos: "el artículo 9.2 consagra el principio de reserva de ley […] previsión no sólo alcanza a las disposiciones que pudieran adoptarse en el futuro, sino que *permite dejar a salvo las distintas habilitaciones legales actualmente existentes*, tal y como se indica específicamente, respecto de la legislación sanitaria y aseguradora, en la disposición adicional decimoséptima dichas habilitaciones, que siguen plenamente vigentes, *permitiendo incluso llevar a cabo una interpretación extensiva de las mismas*, como sucede, en particular, en cuanto al alcance del consentimiento del afectado o el *uso de sus datos sin consentimiento en el ámbito de la investigación biomédica."*

[56] El mismo era previo a la regulación final de la nueva LOPD 3/2018, eso es, que era favorable incluso antes de conocer la regulación final española que es más ventajosa https://www.aepd.es/es/documento/2018-0046.pdf

[57] *Dictamen* CNS 15/2019, de 14.5.2019, Dictamen en relación con la consulta de un centro sanitario sobre la necesidad del consentimiento en el caso de la utilización de datos de salud seudonimizados en investigación biomédica. Disponible en catalán en http://apdcat.gencat.cat/web/.content/Resolucio/Resolucions_Cercador/Dictamens/2019/Documents/ca_cns_2019_015.pdf

Dictamen CNS 18/2019, CNS 18/2019, en relación con la consulta de una asociación del ámbito sanitario sobre diferentes aspectos relacionados con el apartado 2 de la disposición adicional decimoséptima de la Ley Orgánica 3/2018, de 5 de diciembre. Acceso, en catalán, en http://apdcat.gencat.cat/web/.content/Resolucio/Resolucions_Cercador/Dictamens/2019/Documents/ca_cns_2019_018.pdf

[58] COTINO HUESO, L., "El alcance e interactuación del régimen jurídico ... cit..

debe darse partiendo de que la investigación biomédica maneja datos especialmente protegidos que tienen un canon de control y exigencias más elevado.

VIII. ¿CÓMO DEBEN TRATARSE LOS DATOS EN LA INVESTIGACIÓN? LOS PRINCIPIOS DEL TRATAMIENTO DE DATOS

Los pilares estructurales del régimen jurídico de protección de datos han sido y siguen siendo los llamados "principios". Éstos no sólo constituyen **reglas concretas aplicables a los tratamientos, guías esenciales para responsables** y encargados, sino que son **elementos básicos para la interpretación misma de toda la normativa y pauta de actuación por todos** los que traten datos. El artículo 5 RGPD los regula. Así, se afirma que los datos personales serán "a) tratados de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia»)".

Se analizan a continuación los siguientes principios:

1. Licitud del tratamiento
2. Minimización de datos, especialmente en el caso de la investigación. Usar los mínimos datos posibles el menor tiempo
3. Lealtad, información y transparencia
4. Limitación de la finalidad y la posibilidad de usar datos para fines no incompatibles
5. Secreto y confidencialidad
6. Exactitud, corrección y actualización de los datos

Cabe adelantar que se da una grave dificultad para el cumplimiento de los principios básicos de la protección de datos. Así, la finalidad (art. 5.1.b RGPD) de los tratamientos de datos masivos se *desvía* hacia la investigación, cuando no para usos comerciales de los fabricantes, aplicaciones y plataformas. De igual modo, resulta muy difícil prever ulteriores usos de los datos captados. En consecuencia, es muy difícil cumplir con las obligaciones de transparencia e información al interesado (art. 5.1.a y 14.5.b RGPD) frente a usos insospechados al momento de la captación del consentimiento. También, la limitación del plazo de conservación (art. 5.1.e RGPD) pugna con los largos periodos que son naturales a la investigación, donde, además, lo natural es que se encadenen unas y otras investigaciones a partir de los hallazgos de la anterior. Igualmente, el principio esencial de la minimización de datos (art. 5.1.c RGPD) va en contra del mismo concepto de big data o macrodatos que se generan por el uso de inteligencia artificial o IOT, así como contra la necesidad de mayores cantidades de datos para la mayor calidad de la investigación[59]. Además de ir en contra de los principios de la protección de datos, el presupuesto de la

[59] RECUERO LINARES, Mikel, La investigación científica con datos personales genéticos y datos relativos a la salud: perspectiva europea ante el desafío globalizado, Premio AEPD, 2019, pp. 21 y ss. Recuperado de https://www.aepd.es/sites/default/files/2020-02/premio-2019-emilio-aced-accesit-mikel-recuero.pdf

legitimación y consentimiento para la licitud del tratamiento de datos quedan muy modulados en el contexto de inteligencia artificial o IOT e investigación, así como el alcance jurídico y práctico de los derechos de los interesados.

1. Licitud del tratamiento

Por cuanto, a la licitud del tratamiento, de momento baste señalar que cualquier tratamiento de datos solo es lícito si cuenta con consentimiento, o se da en el marco de la ejecución de un contrato, el cumplimiento de una obligación legal se hace para proteger intereses vitales o con fines de interés público o en razón del ejercicio de poder público. Asimismo, un tratamiento justificarse por "intereses legítimos".

2. Minimización de datos, especialmente en el caso de la investigación. Usar los mínimos datos posibles el menor tiempo

El artículo 5 dispone que los datos han de ser "c) **adecuados, pertinentes y limitados a lo necesario** en relación con los fines para los que son tratados («minimización de datos»)".

> El Considerando 39 afirma que "Los datos personales deben ser adecuados, pertinentes y limitados a lo necesario para los fines para los que sean tratados. Ello requiere, en particular, garantizar que se limite a un mínimo estricto su plazo de conservación. Los datos personales solo deben tratarse si la finalidad del tratamiento no pudiera lograrse razonablemente por otros medios. Para garantizar que los datos personales no se conservan más tiempo del necesario, el responsable del tratamiento ha de establecer plazos para su supresión o revisión periódica."

Entre todos los principios, puede decirse que el principio de minimización de los datos adquiere una muy especial relevancia en el RGPD. En buena medida la responsabilidad proactiva y las exigencias para el responsable de la privacidad por defecto y en el diseño vienen a –intentar- garantizar y hacer efectivo el principio de minimización. Baste recordar ahora que el artículo 35.7º sobre Evaluación de impacto relativa a la protección de datos "deberá incluir como mínimo: […] b) una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad."

La Guía de Auditorías de IA 2021 recientemente recuerda la necesidad de:

- preparar los datos personales, depurándolos, aplicando técnicas y buenas prácticas de limpieza de datos
- categorizar los datos en las distintas etapas (no personales, y entre los personales, los que constituyen identificadores, cuasi-identificadores y categorías especiales de datos.
- aplicar los criterios y técnicas de minimización con las estrategias de ocultación, separación, abstracción, anonimización y seudonimización de los datos que sean aplicables

- documentar estas operaciones.-

3. Lealtad, información y transparencia ¿de qué hay que informar? ¿Hay excepciones en el ámbito de la investigación?

El referido artículo 5 RGPD afirma también los principios de lealtad y transparencia, los cuales "exigen que se informe al interesado de la existencia de la operación de tratamiento y sus fines." (Cons. 60).

> "Para las personas físicas debe quedar totalmente claro que se están recogiendo, utilizando, consultando o tratando de otra manera datos personales que les conciernen, así como la medida en que dichos datos son o serán tratados […] en particular a la información de los interesados sobre la identidad del responsable del tratamiento y los fines del mismo y a la información añadida para garantizar un tratamiento leal y transparente con respecto a las personas físicas afectadas y a su derecho a obtener confirmación y comunicación de los datos personales que les conciernan que sean objeto de tratamiento. Las personas físicas deben tener conocimiento de los riesgos, las normas, las salvaguardias y los derechos relativos al tratamiento de datos personales, así como del modo de hacer valer sus derechos en relación con el tratamiento. En particular, los fines específicos del tratamiento de los datos personales deben ser explícitos y legítimos, y deben determinarse en el momento de su recogida." (Cons. 39). Dicha información puede transmitirse en combinación con unos iconos normalizados que ofrezcan, de forma fácilmente visible, inteligible y claramente legible, una adecuada visión de conjunto del tratamiento previsto. Los iconos que se presentan en formato electrónico deben ser legibles mecánicamente." (Cons. 60).

El RGPD contiene a una muy prolija regulación de los deberes de transparencia que se amplían notablemente respecto de la normativa precedente y se concretan en los extensos artículos 12 a 15 que incluyen el propio derecho de acceso. Se trata de una cuestión abordada en la útil Guía para el cumplimiento del deber de informar de la AEPD y las agencias catalana y vasca de 2017.

Guía autoridades de protección de datos sobre transparencia e información.

Imagen de política de privacidad de la AEPD

Epígrafe	Información básica (1ª capa, resumida)	Información adicional (2ª capa, detallada)
"Responsable" (del tratamiento)	Identidad del Responsable del Tratamiento	Datos de contacto del Responsable
		Identidad y datos de contacto del representante
		Datos de contacto del Delegado de Protección de Datos
"Finalidad" (del tratamiento)	Descripción sencilla de los fines del tratamiento, incluso elaboración de perfiles	Descripción ampliada de los fines del tratamiento
		Plazos o criterios de conservación de los datos
		Decisiones automatizadas, perfiles y lógica aplicada
"Legitimación" (del tratamiento)	Base jurídica del tratamiento	Detalle de la base jurídica del tratamiento, en los casos de obligación legal, interés público o interés legítimo.
		Obligación o no de facilitar datos y consecuencias de no hacerlo
"Destinatarios" (de cesiones o transferencias)	Previsión o no de Cesiones	Destinatarios o categorías de destinatarios
	Previsión de Transferencias, o no, a terceros países	Decisiones de adecuación, garantías, normas corporativas vinculantes o situaciones específicas aplicables
"Derechos" (de las personas interesadas)	Referencia al ejercicio de derechos.	Cómo ejercer los derechos de acceso, rectificación, supresión y portabilidad de sus datos, y la limitación u oposición a su tratamiento
		Derecho a retirar el consentimiento prestado
		Derecho a reclamar ante la Autoridad de Control
"Procedencia" (de los datos)	Fuente de los datos (cuando no proceden del interesado)	Información detallada del origen de los datos, incluso si proceden de fuentes de acceso público
		Categorías de datos que se traten

Elementos básicos a informar por el responsable del tratamiento (Guía deber de información).

En **el ámbito más concreto del uso de datos personales para fines de investigación**, como principio hay que informar, máxime teniendo en cuenta que se puede contar con los datos sin un consentimiento del afectado. No obstante, también **pueden relajarse algunas obligaciones de información** (art. 14. 5 b) RGPD). Así, puede exceptuarse el deber de información si ello "resulte imposible o suponga un esfuerzo desproporcionado …, o en la medida en que la obligación […] pueda imposibilitar u obstaculizar gravemente el logro de los objetivos de tal tratamiento. En tales casos, el responsable adoptará medidas adecuadas para proteger los derechos, libertades e intereses legítimos del interesado, inclusive haciendo pública la información"

4. Limitación de la finalidad y la posibilidad de usar datos para fines no incompatibles

El artículo 5.1º b) RGPD regula que los datos han de ser "recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera

incompatible con dichos fines […] («limitación de la finalidad»)". **La adecuación a la finalidad es un eje vertebral de todo tratamiento de datos.**

> No debe olvidarse que un tratamiento puede ser perfectamente lícito y legítimo para una o varias finalidades, pero decae como castillo de naipes en la ilegalidad en cuanto pasa a darse un uso incompatible con la finalidad.

La finalidad pasa a ser esencial para la determinación de su período de conservación.

Y hay que advertir que, aunque se cuente con una causa de legitimización de **un tratamiento** (consentimiento, interés público, etc.), éste **puede pasar a ser ilícito por una desproporción o inadecuación con relación a la finalidad**.

Desproporción puede llevar a que incluso sea ilegal un tratamiento con consentimiento. Incluso el RGPD atisba la posibilidad de que se considere que el consentimiento no ha sido libre y por tanto es nulo si "la ejecución de un contrato, incluida la prestación de un servicio, se supedita al consentimiento al tratamiento de datos personales que no son necesarios para la ejecución de dicho contrato." (art. 7. 4º). Este precepto podría llevar a considerar que no cuentan con la legitimación del tratamiento de datos aquellos servicios –tan habituales en internet- que captan una ingente cantidad de datos que poco o nada tienen que ver con el servicio que brindan al sujeto a cambio de tales datos.

Ahora bien, como **regla general no se considera incompatible usar los datos para la investigación** si se cumplen unos requisitos (art. 5 RGPD)[60]. Así, la regulación flexibiliza y favorece –bajo requisitos- que se puedan destinar a la investigación datos personales recogidos para otros fines o para otras investigaciones. Ello a *cambio* de garantías y "que se disponga de medidas técnicas y organizativas, en particular para garantizar el respeto del principio de minimización de los datos personales."

5. Secreto y confidencialidad

Hay que seguir el principio de integridad y confidencialidad establecido en el art. 5.1.f) RGPD y regulado con alguna mayor concreción en el artículo 5 de la nueva LODP 3/2018[61].

[60] Así, y como principio, el artículo 5 RGPD precisamente cuando afirma el principio de lealtad y finalidad, prevé expresamente que "de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales."

[61] Artículo 5. Deber de confidencialidad.

Este deber de confidencialidad se da en todos los casos y puede añadirse y superponerse a las reglas y exigencias más concretas del mismo, como las regulaciones del secreto profesional, reglas para servidores públicos, secreto industrial, etc. Estas obligaciones se mantendrán aun cuando hubiese finalizado la relación del obligado con el responsable o encargado del tratamiento.

El responsable del tratamiento no sólo debe preocuparse por respetar su propio deber de secreto, también debe asegurarse de que todo el personal a su servicio mantiene la confidencialidad del tratamiento, para lo cual se deben adoptar, al menos, las siguientes medidas[62]:

- Informar al personal de su deber de secreto.
- Adoptar las medidas necesarias para garantizar la confidencialidad de los datos a los que se ha accedido, implantando las medidas técnicas y de carácter organizativo necesarias para impedir que el personal a su servicio pueda revelar datos de carácter personal a terceras personas.
- Firmar compromisos de confidencialidad con todos los usuarios de los sistemas de información con acceso a datos de carácter personal.

6. Exactitud, corrección y actualización de los datos

El artículo 5 RGPD también dispone que los datos serán "d) exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan («exactitud»)". A nadie puede escapar la gravedad e importancia que tiene esta regla para todo responsable o encargado de datos y la responsabilidad activa que conlleva: **"Deben tomarse todas las medidas razonables para garantizar que se rectifiquen o supriman los datos personales que sean inexactos."** Toda empresa, Administración, etc. debe actualizar sus datos de modo que responsan a la realidad[63]. La

1. Los responsables y encargados del tratamiento de datos así como todas las personas que intervengan en cualquier fase de este estarán sujetas al deber de confidencialidad al que se refiere el artículo 5.1.f) del Reglamento (UE) 2016/679.

2. La obligación general señalada en el apartado anterior será complementaria de los deberes de secreto profesional de conformidad con su normativa aplicable.

3. Las obligaciones establecidas en los apartados anteriores se mantendrán aun cuando hubiese finalizado la relación del obligado con el responsable o encargado del tratamiento.

[62] Código de Conducta UNED, 2.6.5. . 13.

[63] En todo caso, la LO 3/2018 en su artículo 4 concreta que no habrá responsabilidad si se adoptan tales medidas razonables para que se supriman o rectifiquen sin dilación cuando los datos inexactos se han obtenido directamente del afectado, cuando se hubiera recibido los datos de otro responsable en virtud del ejercicio por el afectado del derecho a la portabilidad,

gobernanza y la gestión del dato gira en muy buena medida alrededor de estas exigencias. De hecho, la lista de cumplimiento normativo en el ámbito de la UE (Criterios 2019…) y de la reciente Guía de auditoría de la AEPD (p. 23) recuerdan la necesidad de que haya:

- un procedimiento documentado para gestionar y garantizar una adecuada gobernanza de los datos, que permita verificar y aportar garantías de la exactitud, integridad, fiabilidad, veracidad, actualización y adecuación del conjunto de datos utilizado en entrenamiento y/o prueba y/o explotación.
- Supervisión de los procesos de recopilación, tratamiento, conservación y utilización de los datos.
- En el ámbito de la inteligencia artificial resulta especialmente importante el monitoreo de los datos de muestra para entrenamiento, su tamaño y representatividad, la distribución de las variables y que haya procedimientos para detectar posibles desequilibrios.

Cabe recordar que frente a datos inexactos podrá ejercerse el derecho de rectificación o, en su caso, el derecho de supresión u olvido. Y de manera afín, cabe tener en cuenta los derechos digitales de rectificación y de actualización de informaciones (arts. 85-86 LO 3/2018) que, en principio, no quedan al amparo de la autoridad de protección de datos.

cuando el responsable obtuviese del mediador o intermediario cuando las normas aplicables al sector de actividad al que pertenezca el responsable del tratamiento establezcan la posibilidad de intervención de un intermediario o mediador. Tampoco habrá responsabilidad por la inexactitud de los datos obtenidos de un registro público por el responsable.

IX. ¿CUÁNDO SE PUEDEN TRATAR –O CEDER- DATOS? LA "LEGITIMACIÓN" DEL TRATAMIENTO Y LA ESPECIAL FLEXIBILIZACIÓN PARA EL CASO DE LA INVESTIGACIÓN

1. Las vías de legitimación para tratar datos ordinarios y los especialmente protegidos

El punto de partida es que no pueden tratarse datos personales. Y que **sólo se pueden tratar los datos cuando hay una base de legitimación de datos**. Para entendernos, **como si el tratamiento hubiera de estar *bautizado***, de lo contrario se está en el *pecado* de la ilegalidad.

El artículo 6 RGPD[64] determina cómo bautizar los tratamientos de datos.

a) consentimiento libre, inequívoco, específico, informado, acción positiva, que sea demostrable

b) ejecución de un contrato

c)cumplimiento de una obligación legal;

d) intereses vitales

e) misión realizada en interés público o en el ejercicio de poderes públicos (con ley que lo regule)

f) satisfacción de intereses legítimos (con garantías compensatorias)

En esencia, un tratamiento solo es lícito si cuenta con consentimiento, o se da en el marco de la ejecución de un contrato, el cumplimiento de una obligación legal se hace para proteger intereses vitales o con fines de interés público o en razón del ejercicio de poder

[64] El tratamiento solo será lícito si puede enmarcarse dentro de alguna de las siguientes condiciones:

A. El interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos
B. El tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales.
C. El tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento
D. El tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.

público. Asimismo, un tratamiento justificarse por "intereses legítimos". Hay que buscar siempre la base de legitimación y además informar de la misma a los interesados.

Cuando se tratan **datos especialmente protegidos** (ej. salud, genéticos, biométricos, etc.) aún resulta **más difícil *bautizar*** el tratamiento y son mayores los requisitos. Así, la forma de tratarlos legalmente es porque una ley específica así lo permita por causa de "intereses públicos esenciales" o que haya un consentimiento explícito.

2. El régimen de legitimación más flexible para la investigación científica: un cambio de paradigma respecto del consentimiento

En el ámbito de la investigación, la legitimación del tratamiento, esto es, el *bautismo* puede darse por varias vías. Lo natural será lograr el consentimiento de los interesados.

Sin embargo, para la investigación en general, y para en el ámbito del big data y la inteligencia artificial, no resulta nada fácil obtener un consentimiento de los interesados vinculado a una finalidad de investigación que inicialmente ni siquiera se sospecha al momento de la recogida de datos. Cabe recordar que el 4 de mayo 2020 el Comité Europeo de Protección de datos ha actualizado las Directrices sobre el consentimiento[65].

> Para flexibilizar estas dificultades el RGPD (Considerando 33) recuerda que:
>
> "Con frecuencia no es posible determinar totalmente la finalidad del tratamiento de los datos personales con fines de investigación científica en el momento de su recogida. Por consiguiente, debe permitirse a los interesados dar su consentimiento para determinados ámbitos de investigación científica que respeten las normas éticas reconocidas para la investigación científica. Los interesados deben tener la oportunidad de dar su consentimiento solamente para determinadas áreas de investigación o partes de proyectos de investigación, en la medida en que lo permita la finalidad perseguida."

[65] EBDP, *Guidelines 05/2020 on consent under Regulation 2016/679*, Version 1.1. mayo 2020, acceso en https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf

Una versión previa de 2018, en español, en *Directrices sobre el consentimiento en el sentido del Reglamento (UE) 2016/679*, http://www.avpd.euskadi.eus/contenidos/informacion/20161118/es_def/adjuntos/wp259rev01_es20180709.pdf

La **AEPD ha admitido el consentimiento por áreas** en su Informe 073667/20184[66]. Esto puede permitir utilizar los datos de los sujetos para varios proyectos[67].

Pero la flexibilización del régimen jurídico en el caso de la investigación puede llevar a que **no sea necesario el consentimiento** de los interesados de quienes proceden sus datos, **si se dan unas condiciones**. De especial interés para la legitimación en el ámbito de investigación, el Dictamen Autoridad Catalana de Protección de Datos CNS 15/2019. Así, datos que se recogieron para otras finalidades pueden ser utilizados para la investigación. En estos casos, la base de legitimación puede ser variada, en muchos casos será porque hay base legal, esto es, que una ley determina en qué supuestos puede hacerse y fija las condiciones. Ello se combina en algunos casos con la base de legitimación de finalidades públicas, especialmente en el caso de investigaciones del sector público. De igual modo, la base de legitimación de que la investigación es un "interés legítimo", también puede concurrir. Se trata sin duda de una cuestión que requiere de un análisis jurídico y específico.

En principio, es más difícil poder tratar legítimamente **datos especialmente protegidos o sensibles**. No obstante, las finalidades de **investigación científica** son una puerta que flexibiliza el tratamiento de los datos sensibles. Así, el artículo 9. 2 j)[68] permite su tratamiento si hay una regulación específica que lo permita y si se cumplen los requisitos del artículo 89.1 RGPD.

La **nueva LOPD** 3/2018 subraya una visión **favorable y flexibilizadora del uso de datos para la investigación**. Así, su propia exposición de motivos habla de una "interpretación extensiva de las mismas" para el caso de "uso de sus datos sin consentimiento en el ámbito de la investigación biomédica."[69]. La disposición adicional 17ª que más tarde se

[66] https://www.aepd.es/media/informes/2018-0046-investigacionbiomedica.Pdf

[67] Méndez García, Miriam y Alfonso Farnós, Iciar, "La legitimación para el tratamiento de categorías especiales de datos con finalidades de investigación en el marco del Reglamento (UE) 2016/679 y de la Ley Orgánica 3/2018", en *Revista de derecho y genoma humano: genética, biotecnología y medicina avanzada* Nº Extra 1, 2019 (Ejemplar dedicado a: Uso de datos clínicos ante nuevos escenarios tecnológicos y científicos. Oportunidades e implicaciones jurídicas), págs. 205-231, p. 228.

[68] "el tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado."

[69] En concreto lo hace respecto de la regulación existente sobre investigación como válida como base legal para el uso de datos, en especial para el ámbito biomédico"

comenta es buena muestra de ello. Y precisamente en la línea de utilizar datos para finalidades científicas la LO 3/2018 afirma la posibilidad de "reutilización" de datos para la investigación de salud y biomédica (Disposición adicional 17 sobre Tratamientos de datos de salud). En él ámbito más concreto de investigación biomédica, la idea es que se admite la reutilización de los datos de proyectos de investigación preexistentes para ser utilizados en proyectos de investigación relacionados, siempre que se informe adecuadamente al titular de los datos del posterior uso y el proyecto se someta al dictamen del comité de ética[70].

La **AGPD** incluso antes de que se aprobara esta normativa especial, tiene una **visión relativamente favorable a esta tendencia facilitadora**, como se muestra en especial en su Informe 073667/2018[71].

Como más tarde se recuerda, la normativa es más ventajosa a cambio de garantías, como la seudonimización. Una vez sometidos al proceso de anonimización o de seudonimización ya no será preciso el consentimiento para su uso en la investigación. Ahora bien, este proceso es un tratamiento de datos en sí y como tal tratamiento debe estar legitimado. Y hoy día no resulta del todo claro si la seudonimización está directamente permitida por la ley para la investigación o es necesario que interesado de quien se recogen los datos consienta en que se seudonimicen los mismos para investigar. De modo cautelar, cuando se recojan datos e informe para que se preste el consentimiento, es de utilizad informar de que para su uso en la investigación se procederá a su seudonimización[72].

Así, en la Exposición de motivos:

"el artículo 9.2 consagra el principio de reserva de ley […] previsión no sólo alcanza a las disposiciones que pudieran adoptarse en el futuro, sino que *permite dejar a salvo las distintas habilitaciones legales actualmente existente***s**, tal y como se indica específicamente, respecto de la legislación sanitaria y aseguradora, en la disposición adicional decimoséptima

dichas habilitaciones, que siguen plenamente vigentes, *permitiendo incluso llevar a cabo una interpretación extensiva de las mismas*, como sucede, en particular, en cuanto al alcance del consentimiento del afectado o el *uso de sus datos sin consentimiento en el ámbito de la investigación biomédica."*

[70] Méndez García, Miriam y Alfonso Farnós, Iciar, "La legitimación para el tratamiento de categorías especiales de datos con finalidades de investigación en el marco del Reglamento (UE) 2016/679 y de la Ley Orgánica 3/2018", en *Revista de derecho y genoma humano: genética, biotecnología y medicina avanzada* Nº Extra 1, 2019 (Ejemplar dedicado a: Uso de datos clínicos ante nuevos escenarios tecnológicos y científicos. Oportunidades e implicaciones jurídicas), págs. 205-231, p. 228-229.

[71] El mismo era previo a la regulación final de la nueva LOPD 3/2018, eso es, que era favorable incluso antes de conocer la regulación final española que es más ventajosa https://www.aepd.es/es/documento/2018-0046.pdf

[72] Considera que sí que es necesario el consentimiento para la anonimización o de seudonimización Romeo Casabona Carlos María, "Revisión de las categorías jurídicas de la

Obligaciones de informar de la legitimación: En el momento de recoger los datos de los interesados, en las cláusulas informativas elaboradas al efecto, debe incluirse la base legal sobre la que se desarrolla el tratamiento. Si no se ha necesitado el consentimiento, habrá igualmente que informar de la base de legitimación que permite el tratamiento (por ejemplo, la legislación que permite que no se exija consentimiento).

Asimismo, en el **Registro de Actividades de Tratamiento** hay que identificar las bases legales aplicables en cada caso concreto.

Sobre esta base, lo normal será que, en los procedimientos internos de comunicación o solicitud de autorización dentro de las organizaciones para tratamientos de datos, se comunique lo que se considera que es la base de legitimación del tratamiento de datos. No obstante, se trata de una cuestión que necesariamente debe pasar por la evaluación jurídica.

Así, lo habitual será indicar una de las vías de legitimación del tratamiento que correspondan, o varias:

- Consentimiento del interesado
- Cumplimiento de una obligación legal
- Misión realizada en interés público
- Ejecución de un contrato Aplicación de medidas
- precontractuales
- Protección de intereses vitales
- Interés legítimo
- Ejercicio de poderes públicos
- Tratamiento de una categoría especial de datos

El cambio de paradigma que se da en salud e investigación en salud merced a la inteligencia artificial, big data o el internet de las cosas y la sensorización (IOT) se traduce en un cambio en los tradicionales modelos de consentimiento[73]. Hay un nuevo enfoque basado en el control eficiente por las autoridades del uso de los datos a partir de un

normativa europea ante la tecnología del big data aplicada a la salud", *Revista de derecho y genoma humano: genética, biotecnología y medicina avanzada* Nº Extra 1, 2019 (Ejemplar dedicado a: Uso de datos clínicos ante nuevos escenarios tecnológicos y científicos. Oportunidades e implicaciones jurídicas), págs. 85-128, p. 110.

[73] MONTALVO JÄÄSKELÄINEN, Federico, "Una reflexión desde la teoría de los derechos fundamentales sobre el uso secundario de los datos de salud en el marco del Big Data", *Revista de Derecho Político*, nº 106, 2019, pp. 43-75, ver pp. 56, 59 y en especial p. 69.

consentimiento inicial y un origen legítimo de los datos.[74] Se ha pasado en general a permitir un "consentimiento amplio" o "*broad consent*" para ulteriores usos. Ello conlleva graves problemas de información y transparencia al consentir para fines indeterminados y la pérdida la capacidad de control sobre los mismos, como recuerdan Recuero y Bonnie[75]. La tendencia es que los datos se puedan reutilizar "para las mismas líneas de investigación", entendidas ampliamente las posibles líneas de investigación (por ejemplo, genéricamente, el cáncer[76]. En esta línea el Consejo de Europa afirma que "los interesados deben poder expresar su consentimiento para ciertas áreas de investigación o ciertas partes de proyectos de investigación, en la medida permitida por el propósito previsto, con el debido respeto a los estándares éticos reconocidos." (punto 15.6)[77]. En España, la DA 17º 2º LO 3/2018 flexibiliza el consentimiento informado y si los datos pasan a ser seudonimizados admite que se puedan reutilizar para áreas de investigación afines y diversos proyectos. La AEPD ha admitido el consentimiento por áreas en su Informe 073667/20184.

3. Un consentimiento explícito, probado, revocable y concurrente con otros consentimientos en el ámbito biomédico

Debe recordarse que, si la base de legitimación es el consentimiento y se trata de datos especialmente protegidos, se precisa un consentimiento explícito.

Una vía de garantizar este carácter explícito es que sea por escrito y con firma del interesado para eliminar dudas de prueba. En el contexto digital que será el más habitual respecto del uso de inteligencia artificial, big data o el internet de las cosas, es posible el consentimiento explícito al rellenar un impreso electrónico, completar plantillas que pidan confirmación específica del interesado y ofrezcan enlaces de confirmación que confirmen

---

[74] ROMEO CASABONA, Carlos María, "Revisión de las categorías jurídicas de la normativa europea ante la tecnología del big data aplicada a la salud", en *Revista de derecho y genoma humano: genética, biotecnología y medicina avanzada* nº Extra 1 *Revista de derecho y genoma humano: genética, biotecnología y medicina avanzada* Nº Extra 1, 2019, pp. 85-127, p. 127.

[75] RECUERO LINARES, Mikel, La investigación científica con datos… cit. p. 29.

[76] GERMAN ETHICS COUNCIL, *Big Data and Health – Data Sovereignty as the Shaping of Informational Freedom, Opinion · Executive Summary & Recommendations*, 30 de noviembre 2017, punto 16. Deutscher Ethikrat, Berlin, disponible en https://www.ethikrat.org/fileadmin/Publikationen/Stellungnahmen/englisch/opinion-big-data-and-health-summary.pdf También, MONTALVO JÄÄSKELÄINEN, Federico, "Una reflexión … cit. pp. 69 y ss.

[77] CONSEJO DE EUROPA, Recomendación CM / Rec (2019) 2 del Comité de Ministros a los Estados miembros sobre la protección de datos relacionados con la salud, de 27 de marzo 2019

Disponible en
https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=090000168093b26e

su autorización. Asimismo, es posible un correo electrónico y contestación específica, un documento escaneado con firma o con firma electrónica. No hay que excluir formulas verbales siempre que quede constancia.[78]

Respecto de la legitimación por consentimiento, además de las exigencias de que éste sea explícito, hay que tener en cuenta que en el contexto de servicios de salud e investigación biomédica es muy posible un claro desequilibrio entre las partes, lo cual conllevaría un consentimiento que no es libre (art. 7.4º RGPD)[79]. Este problema de asimetría consiguiente viciada legitimación para el tratamiento de datos relacionados con la salud es si cabe más acuciante respecto de los tratamientos masivos por plataformas, redes y fabricantes.

Cabe recordar asimismo que el consentimiento de protección de datos ha de poder revocarse con la misma sencillez que se prestó (art. 7 RGPD). Ahora bien, hay que tener en cuenta que en muchos supuestos el tratamiento de datos por tecnologías disruptivas no se legitima por el consentimiento, sino en la ley o en el contrato. Así, es muy posible que de haber una revocación del consentimiento no tenga efectos especialmente respecto del tratamiento de datos primario de salud. Si se da una revocación, el responsable del tratamiento deberá detener las operaciones de tratamiento en cuestión que se fundamentaban en el consentimiento, pero no las basadas en el contrato que sigue vigente o las vías de legitimación que son habituales en el ámbito de salud e investigación. Obviamente, si no existe ningún otro fundamento lícito que justifique la retención para un tratamiento posterior, el responsable del tratamiento deberá suprimir los datos (art. 17.1.b y 3 RGPD)[80].

Además del consentimiento en razón del régimen de protección de datos, el consentimiento informado es exigible por la dignidad de la persona (art. 10. 1º CE que se desarrolla en las leyes de autonomía del paciente) para el ámbito de los tratamientos de salud. Y este mismo consentimiento se exige para la investigación biomédica y los ensayos clínicos, según concreta la diferente legislación. Pues bien, pese a que estos consentimientos se recaban por lo general en el mismo momento, son diferentes[81].

---

[78] *Ibídem*, sobre el consentimiento explícito pp. 20-22.

[79] CONSEJO DE EUROPA, *Recomendación CM / Rec (2019) … cit.* en esta dirección en su punto 18 afirma que "además, el consentimiento no debe constituir un fundamento jurídico válido para el tratamiento de datos personales en un caso concreto en el que exista un claro desequilibrio entre el interesado y el responsable del tratamiento". Recuerda que "pueden producirse situaciones de desequilibrio de poder entre el patrocinador/investigador y los participantes" (punto 19), no será libre "cuando un participante no esté en buenas condiciones de salud, cuando los participantes pertenezcan a un grupo desfavorecido económica o socialmente o en cualquier situación de dependencia institucional o jerárquica" (punto 20).

[80] CONSEJO DE EUROPA, Recomendación CM / Rec (2019) … cit. punto. 20.

[81] Ver punto 15 y (nº 29). "el consentimiento previsto en el párrafo 2 del artículo 28 del CTR no es el mismo consentimiento al que se hace referencia en la RBP como uno de los fundamentos

Las herramientas informáticas y aplicaciones IOT que recogen datos relacionados con la salud es posible que no impliquen un tratamiento de datos personales sujeto a la normativa, bien porque se recojan forma totalmente anonimizada, bien porque queden bajo la excepción doméstica[82]. Sin embargo, pese a que no haya un tratamiento de datos sujeto a legitimación, el consentimiento puede ser exigible por la Directiva de privacidad en las comunicaciones (artículos 5 y 9 Directiva 2002/58/CE) cuando haya una lectura de datos del dispositivo, una instalación de información en el terminal del interesado o acceso a datos de geolocalización[83].

Así las cosas, son muchos los caminos que conducen a la *Roma* del consentimiento, si bien el consentimiento puede tener diferentes regímenes jurídicos que habrán de cumplirse en el ámbito de las tecnologías inteligencia artificial, big data y conexas.

4. Un nuevo paradigma del uso de datos primarios y secundarios big data en la investigación

Como se ha adelantado, hay un auténtico *tsunami* o aluvión de datos e información relacionados con la salud, por lo general desestructurados, procedentes del uso masivo de tecnologías disruptivas

Y además estas fuentes crecientes de datos masivos pueden quedar fácilmente vinculadas a contextos de uso para la investigación. Y ello se da cada vez más en razón del crecimiento de la investigación aplicada (*translational research*) o *bench to bedside* (del laboratorio a la cabecera del enfermo), de la demanda de "trasladar los hallazgos del laboratorio o la universidad a los hospitales, centros de salud y la medicina clínica"[84]. Otros factores también llevan a un cambio de paradigma: los datos asociados a los usos

---

jurídicos del tratamiento de los datos personales, independientemente de que sea o no el fundamento jurídico utilizado para el tratamiento primario"

COMISIÓN EUROPEA, *Question and Answers on the interplay between the Clinical Trials Regulation and the General Data Protection Regulation*, Dirección General de Salud e Inocuidad de los Alimentos, 2019. Disponible en https://ec.europa.eu/health/human-use/clinical-trials-documents_es,

[82] Cabe recordar que se dará la excepción doméstica y por tanto no aplicará la normativa de protección de datos "Si el procesamiento de datos sólo tiene lugar en el propio dispositivo, y no se transmiten datos personales fuera del dispositivo, la ley no se aplicaría al usuario, debido a la excepción para el uso puramente personal". Así, Anexo Carta del Grupo del artículo 29 sobre el ámbito del tratamiento de datos de salud por app a petición de la Comisión Europea de 5 de febrero de 2015 https://ec.europa.eu/justice/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_annex_en.pdf

[83] Ibídem.

[84] ÁNGELES CASTELLANOS, Manuel; ESCOBAR, Carolina. "Medicina traslacional". *Revista de la Facultad de Medicina de la UNAM* [en línea]. Madrid: UNAM, vol. 59, nº 2, 2016, pp. 15-23, p. 16: 19/07/2019. Disponible en: https://www.medigraphic.com/pdfs/facmed/un-2016/un162c.pdf

primarios de los servicios de salud se utilizan para la investigación, hay un crecimiento exponencial de estas tecnologías asociado tanto a los servicios de salud, así como en razón del uso y acceso a datos relacionados con la salud por plataformas, redes y los más variados productos IOT. Y a todo ello se une un uso secundario, ya para la investigación médica, ya para otros usos comerciales por las plataformas, redes y fabricantes. Hoy día es "prácticamente inexistente" la investigación que no se sirve del tratamiento de datos obtenidos de diversas fuentes[85].

Así pues, el esquema general es que el paciente cede sus datos para un fin concreto primario (el servicio de salud) y tales datos cobran interés para fines secundarios, su uso secundario, a través de las herramientas que ofrece el Big Data."[86] Estas dos esferas que antaño estaban mucho más distanciadas y que tenían un régimen jurídico también más diferenciado hoy se superponen. Y jurídicamente las posibilidades de estos usos secundarios dependen de muchos factores.

5. Las cesiones o comunicaciones de datos a terceros

La comunicación de datos a terceros es un tratamiento de datos que en principio está prohibido y requiere también una base de legitimación, estar *bautizada*. En general, se podrá comunicar datos cuando una Ley obliga a ello o el interesado consienta.

El acceso a datos por corresponsables de datos o por encargados, no son comunicaciones de datos,

Como se ha subrayado en el apartado relativo a la gobernanza y las figuras de responsable y encargado, en los procedimientos internos en las organizaciones y desde el inicio hay que tener clara una estrategia que incluya la previsión de la comunicación de datos. Así, por ejemplo, cabe tener en cuenta supuestos de diversos responsables de conjuntos estructurados datos. Cabe también recordar que tratar datos en nombre de otro para prestar servicios en el marco de un contrato, subvención, etc. no es una comunicación de datos, sino que sigue el régimen y responsabilidades de responsable y encargado de datos personales.

[85] ALKORTA IDIAKEZ, Itziar, , "Regulación del tratamiento de los datos en proyectos de investigación sanitaria, en especial, en la aplicación de las tecnologías Big data", en *Revista de derecho y genoma humano: genética, biotecnología y medicina avanzada* Nº Extra 1, 2019, pp. 273-323, p. 274.

[86] MONTALVO JÄÄSKELÄINEN, Federico, "Una reflexión desde la teoría... cit. , pp. 47-48.

En cualquier caso, desde el inicio cabe intentar prever las cesiones o comunicaciones de datos. Así, los procedimientos internos suelen requerir calificar la Tipificación de los destinatarios de los datos:

- Administración pública con competencia en la materia
- Entidades aseguradoras
- Organizaciones o personas directamente relacionadas
- Administración tributaria
- Entidades sanitarias
- Otros órganos de la Administración Pública
- Asociaciones y organizaciones sin ánimo de lucro
- Fuerzas y Cuerpos de Seguridad
- Prestaciones de servicios de telecomunicaciones
- Entidades financieras
- Notarios
- Sindicatos y juntas de personal
- Colegios profesionales
- Registros públicos
- Prestadores de servicios externalizados
- Autoridades de control (AEPD, CNMV etc.)
- Empresas dedicadas a publicidad o marketing
- Organismos de la seguridad social
- Organismos de la Unión Europea
- Otros (Indicar cuáles).

Facilidad para las cesiones de datos para investigaciones y estudios científicos en el sector público

La CRUE (Conferencia de Rectores de las Universidades Españolas) ha realizado algunas indicaciones en su reciente *Guía de buenas prácticas* en materia de Transparencia y Protección de Datos[87].

De una parte, respecto de la **Cesión de datos entre administraciones para estudios científicos** (pp. 35 y ss.) se afirma que si el tratamiento de datos se vincula a "un estudio incardinado en un proyecto institucional su título legitimador sería el art. 6.1.e) RGPD, sin que sea necesario, por consiguiente, con carácter general, el consentimiento del titular de los datos, dado que se produce entre Administraciones públicas y tiene como objeto su tratamiento posterior con finalidad de carácter científico (por todos, informe AEPD 9901/2002).

Si se trata de una **comunicación de datos especialmente protegidos** (como, por ejemplo, datos de salud) se ha de solicitar el previo consentimiento expreso del interesado, con independencia de que el trabajo a desarrollar se inserte o no en el marco de un proyecto institucional (informe 0317/2009).

Sin embargo, señala la AEPD que si lo que se pretende con la comunicación es el tratamiento ulterior de los datos personales con **fines estadísticos**, el estudio tendría que ser considerado como estadística de cumplimentación obligatoria a los efectos previstos en la Ley 12/1989, de 9 de mayo, de la Función Estadística Pública, o legislación autonómica correspondiente[88] En caso contrario, se necesitaría el previo consentimiento de los afectados (informe 0379/2009).

[87] Pp. 33 y ss.

[88] Véase asimismo el dictamen CNS 49/2018 de la APDCat.

X ¿PARA QUÉ FINALIDADES SE PUEDEN MANEJAR O TRATAR DATOS? EL USO EN LA INVESTIGACIÓN

Investigar en ecosistemas de investigación i-Spaces como Data Space comporta el manejo de datos, este manejo jurídicamente se le denomina "tratamiento" ("cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no).

1. ¿Se pueden usar datos para otras finalidades que las inicialmente previstas?

Según se ha adelantado (artículo 5.1º b) RGPD) regula que los datos han de ser "recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines […] («limitación de la finalidad»)". Y hay que advertir que **lo prohibido son los usos "incompatibles",** no las finalidades distintas: "El tratamiento de datos personales con fines distintos de aquellos para los que hayan sido recogidos inicialmente solo debe permitirse cuando sea compatible con los fines de su recogida inicial." (Cons. 50) Recuerda el RGPD que, para admitir nuevos fines, "no se requiere una base jurídica aparte, distinta de la que permitió la obtención de los datos personales" (Cons. 50). Y es que, si hay un cambio de finalidades, pero las mismas cuentan con una base de legitimación (consentimiento, ley, etc.) no habría problema.

Ciertamente en el entorno de la Inteligencia Artificial y tecnologías conexas se hace casi imposible determinar previamente las finalidades concretas para las que se van a utilizar los datos. De ahí la especial necesidad de flexibilización en el ámbito de investigación que aquí interesa. En cualquier caso, interesará tener documentados los objetivos (iniciales) de lo que se pretende, contextualizando las dinámicas, actividades y/o procesos en el marco de la organización en la que se integra la etapa del ciclo de vida del componente IA.

En los procedimientos internos de comunicación –autorización de tratamientos, será habitual la obligación de comunicar el fin o los fines para los que se quiere tratar datos.

Así, por ejemplo, pueden seguirse las finalidades y usos previstos estandarizados o tipificados en el Reglamento del registro de actividades de tratamiento de la Universitat Politècnica de València:

- Análisis de perfiles
- Gestión de clientes, contable, fiscal y administrativa
- Gestión de proveedores,
- Gestión y control sanitario
- Información electoral y de Comercio electrónico
- Control de uso de servicios e instalaciones compras e información económica
- Gestión de información de colectivos, organizaciones o asociaciones sindicatos de estudiantes
- Inscripción a jornadas y eventos
- Convocatorias y oposiciones

- Gestión de información de estudios y encuestas
- Minería de datos
- Cumplimiento/Incumplimiento de obligaciones
- Gestión de ayudas y subvenciones
- Prevención de riesgos laborales
- Difusión de información académica e institucional
- Gestión de incidencias de soportes informáticos
- Promoción de empleo e inserción profesional
- Evaluación de calidad
- Gestión de las solicitudes de ejercicio de derechos personales
- Publicidad y prospección comercial
- Fines estadísticos, históricos o científicos. Proyectos de investigación.
- Gestión y evaluación académica
- Recursos Humanos
- Gestión de jornadas/congresos
- Gestión de actividades asociativas, culturales…
- Gestión de información de participantes y ponentes en congresos, jornadas y seminarios
- Gestión de proyectos, programas y cursos formativos
- Gestión de información jurídica, recursos o reclamaciones administrativas
- Gestión de peticiones/sugerencias de información
- Gestión de información los medios de comunicación (RTV y prensa)
- Gestión de información bibliotecaria
- Registro de entradas y salidas de documentos
- Registro de delegaciones de firma y competencia
- Seguridad privada
- Seguridad y control de acceso a edificios
- Gestión de TFG, TFM y tesis doctorales
- Gestión y emisión de nóminas
- Servicios relacionados con la minería de datos
- Tramitación de expedientes o certificados, títulos, diplomas o premios
- Gestión de información de las escuelas, laboratorios u otros centros
- Gestión de asistencia social
- Gestión de información de procedimientos administrativos
- personas menores de 14 años
- Videovigilancia
- Gestión de alumnos, futuros alumnos o antiguos alumnos
- Gestión de usuarios web

- Gestión o evaluación de trabajadores
- Gestión de prácticas

2. ¿Cuándo un uso de datos es incompatible con la finalidad inicial?

Es posible que los datos que se tienen inicialmente recogidos para una finalidad quieran utilizarse para otras finalidades. En estos casos**, la clave es determinar si el desvío de finalidad en el tratamiento de datos es aceptable o se trata de un prohibido uso incompatible.**

La posibilidad de usar datos para fines no incompatibles es una cuestión jurídica y técnica que debe ser puesta en conocimiento de la organización para efectuar una evaluación de incompatibilidad.[89] Como punto de partida, el G29 señala que en los supuestos en los que la compatibilidad resulta obvia, no habrá que hacer mayor esfuerzo y análisis. Sin embargo, en otros casos no será obvia la compatibilidad entre la finalidad para la que se recogieron los datos y a lo que se destina. Así ha de analizarse con intensidad y profundidad el supuesto[90].

En este análisis son muchos los factores a tener en cuenta. Este juicio de incompatibilidad consiste en definir la finalidad o finalidades iniciales y determinar la adicional o nueva finalidad. Obviamente, a mayor distancia entre la finalidad original y la adicional, más difícil será sostener la relación de compatibilidad. Hay que atender a la realidad y contexto

[89] Al respecto cabe tener especialmente en cuenta la Opinión 3/2013 del Grupo del Artículo 29 que detalla el análisis jurídico, un test o juicio de la incompatibilidad que se hace caso por caso bajo una serie de parámetros y con diferentes intensidades.

[90] Este juicio de compatibilidad en buena medida ha sido recogido en el artículo 6. 4 RGPD:

“el responsable del tratamiento, con objeto de determinar si el tratamiento con otro fin es compatible con el fin para el cual se recogieron inicialmente los datos personales, tendrá en cuenta, entre otras cosas:

a) cualquier relación entre los fines para los cuales se hayan recogido los datos personales y los fines del tratamiento ulterior previsto;

b) el contexto en que se hayan recogido los datos personales, en particular por lo que respecta a la relación entre los interesados y el responsable del tratamiento;

c) la naturaleza de los datos personales, en concreto cuando se traten categorías especiales de datos personales, de conformidad con el artículo 9, o datos personales relativos a condenas e infracciones penales, de conformidad con el artículo 10;

d) las posibles consecuencias para los interesados del tratamiento ulterior previsto;

e) la existencia de garantías adecuadas, que podrán incluir el cifrado o la seudonimización.”

del caso concreto, analizar si había expectativas razonables desde el inicio de que los datos serían usados para fines adicionales; hay que tener en cuenta la legitimidad de base (consentimiento, contrato, interés legítimo, etc.). Se ha de apreciar qué garantías se dieron en aquel momento inicial. No hay que obviar la real capacidad de elección o consentimiento del interesado, la relación que se da entre responsable e interesado, la asimetría que puede darse entre ambos, la naturaleza, cualidad y capacidad del responsable. Asimismo, el análisis de compatibilidad también exige tener en cuenta el impacto efectivo y real, así como en la percepción, del propio afectado por el cambio de finalidad. También hay que tener en cuenta si en el nuevo tratamiento entran nuevos sujetos, nuevas comunicaciones de datos a terceros, etc. Resulta clave en la valoración precisar si se ha compensado el desvío de la finalidad con garantías para el interesado, especialmente a través de buena información y mecanismos efectivos para el ejercicio de sus derechos ante el desvío de finalidad.

Sin perjuicio del régimen de investigación que ahora se comenta, será más fácil considerar la compatibilidad del tratamiento de datos que se realiza en entornos de investigación, especialmente si es pública.

3. Usar datos para la investigación en general no es un uso incompatible

En el ámbito de entidades de investigación en su caso universitarias y ecosistemas como Data Space no será nada extraño que los datos inicialmente recogidos para una finalidad quieran utilizarse para otras finalidades, o para otras investigaciones. Como ya se ha adelantado que la regulación facilita la legitimación de tratamientos de datos para investigar, así como exceptúa o relaja algunas de sus obligaciones para facilitar la investigación.

Por lo que ahora interesa, como **regla general no se considera incompatible usar los datos para la investigación** si se cumplen unos requisitos (art. 5 RGPD)[91]. Así, la regulación flexibiliza y favorece –bajo requisitos- que se puedan destinar a la investigación datos personales recogidos para otros fines o para otras investigaciones. La regulación más específica se ha dado para la investigación biomédica que ahora se comenta. No obstante, debe tenerse en cuenta lo afirmado respecto de la facilidad de considerar compatibles usos para la investigación, especialmente si hay un análisis de riesgos, estudios de impacto, garantías, etc.

[91] Así, y como principio, el artículo 5 RGPD precisamente cuando afirma el principio de lealtad y finalidad, prevé expresamente que “de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales.”

4. Tratamiento de datos en la investigación en salud o biomédica

No es lugar ahora de analizar extensamente el régimen jurídico de protección de datos en la investigación y en concreto en la biomédica[92]. El RGPD es consciente del valor público y social de la investigación, excepciona, flexibiliza o relaja algunas de las exigencias de protección de datos *a cambio* de "garantías adecuadas" (artículo 89. 1º RGPD, ver en especial Considerandos 33 y 157 y en particular los artículos 5 y 9 RGPD). El artículo 9 sobre datos especialmente protegidos flexibiliza la necesidad de consentimiento para el uso científico y de investigación de datos, vinculándolo al referido artículo 89 y también fija algunos requisitos. Así, en el ámbito de salud y de investigación en salud, son de especial interés los apartados g) h), i) del RGPD y en particular relación con la investigación, la letra j), vinculada al referido artículo 89 RGPD[93]. El principio de minimización pasa a primer plano y las técnicas de seudonimización son la piedra angular, de modo que "que no permita o ya no permita la identificación de los interesados" (art. 89 RGPD). Así, el RGPD ha establecido un marco y unos mínimos desarrollados en la LO 3/2018, en particular en su Disposición adicional 17ª (DA 17ª).

Según ya se ha adelantado respecto de las bases de legitimación, el artículo 9 RGPD sobre datos especialmente sensibles (como los de salud, biométricos, etc.) flexibiliza la

---

[92] Sobre el tema, cabe destacar el Premio Emilio ACED 2019, RECUERO LINARES, Mikel, La investigación científica con datos personales genéticos y datos relativos a la salud: perspectiva europea ante el desafío globalizado, Premio AEPD, 2019, pp. 21 y ss. Recuperado de https://www.aepd.es/sites/default/files/2020-02/premio-2019-emilio-aced-accesit-mikel-recuero.pdf

Sobre el tema de big data en salud e investigación biomédica en España destacan, por todos, los diversos estudios en el monográfico *Revista de derecho y genoma humano: genética, biotecnología y medicina avanzada* Nº Extra 1 (Ejemplar dedicado a: Uso de datos clínicos ante nuevos escenarios tecnológicos y científicos. Oportunidades e implicaciones jurídicas), 2019; SAN SEGUNDO ENCINAR, José María (Dir.), *Big data en salud digital*. Fundación Vodafone, MINETAD, RED.ES, Madrid, 2017; MONTALVO JÄÄSKELÄINEN, Federico, "Una reflexión desde la teoría de los derechos fundamentales sobre el uso secundario de los datos de salud en el marco del Big Data", *Revista de Derecho Político*, nº 106, 2019, pp. 43-75; TRONCOSO REIGADA, A. "Investigación, salud pública y asistencia sanitaria en el Reglamento General de Protección de Datos de la Unión Europea y en la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales, en *Revista de derecho y genoma humano,* nº 49, 2018 o MARTÍNEZ MARTÍNEZ, Ricard, "Big data, investigación en salud y protección de datos personales: ¿Un falso debate?", en *Revista valenciana d'estudis autonòmics*, nº 62, 2017, pp. 235-280 o COTINO HUESO, L. "El alcance e interactuación del régimen jurídico … cit.

[93] "j) el tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado."

necesidad de consentimiento para el uso científico de datos, vinculándolo al referido artículo 89. Y también en la LO 3/2018 resulta significativa la legalización o afirmación de compatibilidad que se ha dado respecto de la "reutilización" de datos para la investigación de salud y biomédica (Disposición adicional 17 sobre Tratamientos de datos de salud).

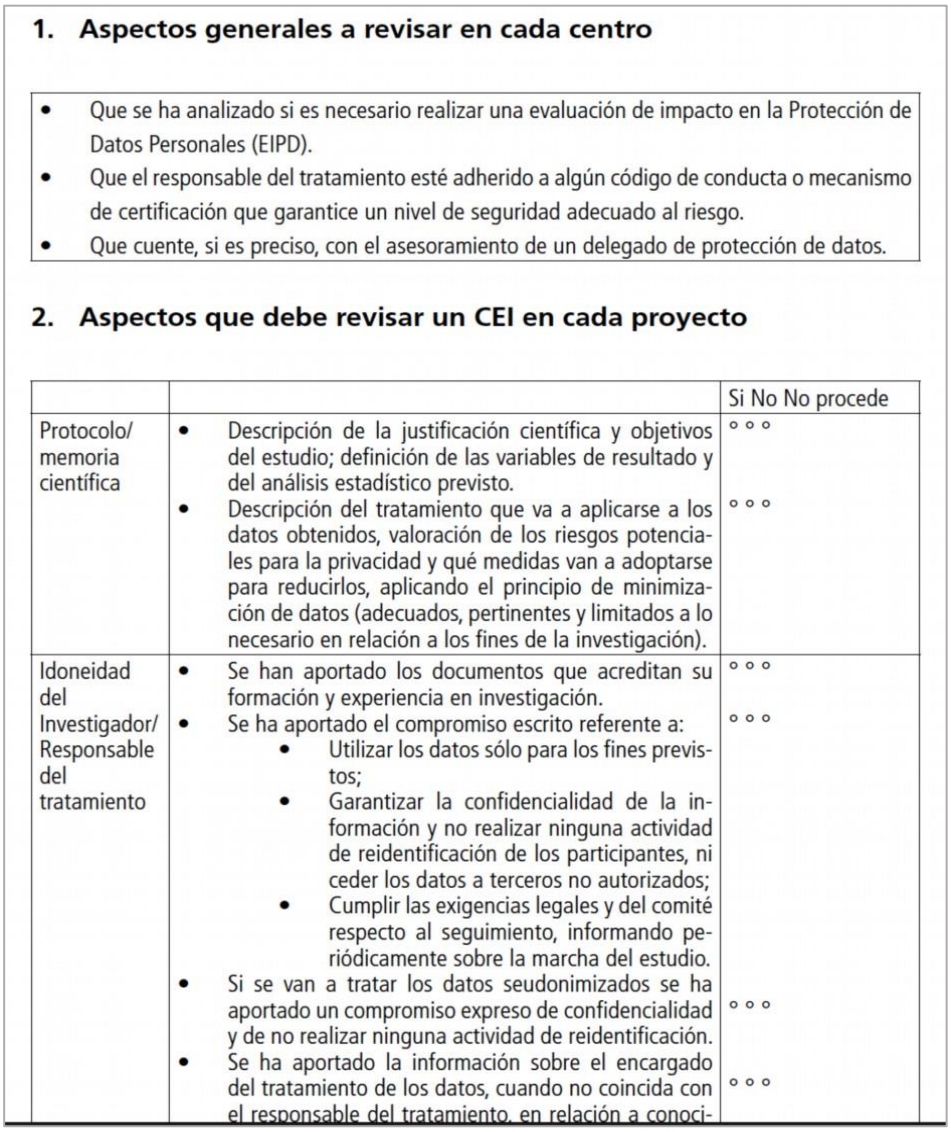
El tratamiento de datos para el ámbito de salud –e investigación biomédica- merece una especial atención y cabe remitir a algunos estudios extensos al respecto.

Procede, en todo caso, delimitar que en la línea de lo concretado por la autoridad catalana "La referencia a la "**salud pública**" contenida en la letra b) del apartado 2 de la DA 17ª, **debe entenderse** hecha a la investigación que se lleve a cabo en el marco de la Ley 33/2011, de 4 de octubre, General de Salud Pública, en cambio, las previsiones de las letras d) f) y g) se entenderán referidas a cualquier investigación en salud.

En todo caso debe partirse de que se da la general flexibilización que confiere el RGPD para la investigación y un especial régimen favorable en la LO 3/2018. Así se expresa en su exposición de motivos y en particular en la regulación especial de la disposición adicional decimoséptima. También hay que tener en cuenta diversas normas específicas y en particular la Ley 14/1986, de 25 de abril, General de Sanidad, encaminados a garantizar el adecuado desarrollo de la investigación en materia de salud, y en particular la biomédica, ponderando los indudables beneficios que la misma aporta a la sociedad con las debidas garantías del derecho fundamental a la protección de datos.

Al respecto de este tema, resulta de especial utilidad el "**Cuestionario/guía para la evaluación de proyectos de investigación con datos por un CEI** (En cumplimiento del Reglamento Europeo 2016/679 de protección de datos y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales)[94]. El mismo se reproduce en el **anexo**.

[94] Alfonso Farnós, Iciar Alcalde Bezhold, Guillermo y Méndez García Miriam, en *Revista de derecho y genoma humano* Nº Extra 1, 2019 (Ejemplar dedicado a: Uso de datos clínicos ante nuevos escenarios tecnológicos y científicos. Oportunidades e implicaciones jurídicas), págs. 25-33.



1. Aspectos generales a revisar en cada centro

- Que se ha analizado si es necesario realizar una evaluación de impacto en la Protección de Datos Personales (EIPD).
- Que el responsable del tratamiento esté adherido a algún código de conducta o mecanismo de certificación que garantice un nivel de seguridad adecuado al riesgo.
- Que cuente, si es preciso, con el asesoramiento de un delegado de protección de datos.

2. Aspectos que debe revisar un CEI en cada proyecto

		Si No No procede
Protocolo/ memoria científica	• Descripción de la justificación científica y objetivos del estudio; definición de las variables de resultado y del análisis estadístico previsto. • Descripción del tratamiento que va a aplicarse a los datos obtenidos, valoración de los riesgos potenciales para la privacidad y qué medidas van a adoptarse para reducirlos, aplicando el principio de minimización de datos (adecuados, pertinentes y limitados a lo necesario en relación a los fines de la investigación).	° ° ° ° ° °

Idoneidad del Investigador/ Responsable del tratamiento	• Se han aportado los documentos que acreditan su formación y experiencia en investigación.
	• Se ha aportado el compromiso escrito referente a:
	  • Utilizar los datos sólo para los fines previstos;
	  • Garantizar la confidencialidad de la información y no realizar ninguna actividad de reidentificación de los participantes, ni ceder los datos a terceros no autorizados;
	  • Cumplir las exigencias legales y del comité respecto al seguimiento, informando periódicamente sobre la marcha del estudio.
	• Si se van a tratar los datos seudonimizados se ha aportado un compromiso expreso de confidencialidad y de no realizar ninguna actividad de reidentificación.
	• Se ha aportado la información sobre el encargado del tratamiento de los datos, cuando no coincida con el responsable del tratamiento, en relación a conoci-
		° ° °
		° ° °
		° ° °
		° ° °

Imagen del Cuestionario/guía para la evaluación de proyectos de investigación con datos por un CEI.

Asimismo, cabe remitirse a lo afirmado y recomendado por la **CRUE en su Guía de buenas prácticas**[95] que a continuación se reproduce.

"El legislador ha considerado incluidos en los supuestos de las letras g), h), i) y j) del artículo 9.2 RGPD a los tratamientos de datos relacionados con la salud regulados en la normativa de salud pública, pero estableciendo unas consideraciones específicas respecto de los estudios científicos que puedan llevar- se a cabo con dichos datos de salud, para los cuales no será necesario contar con el consentimiento de las personas afectadas, cuando se trate de situaciones de excepcional relevancia y gravedad para la

[95] P. 36 y ss.

salud pública, no por tanto cuando no se den estas circunstancias –apartado 2.b) de la disposición adicional decimoséptima LOPDGDD-.

Por ello, no dándose los supuestos previstos anteriormente, será necesario el consentimiento del interesado o, en su caso, de su representante legal para el uso de sus datos con fines de investigación en salud y, en particular, la biomédica. Tales finalidades podrán abarcar categorías relacionadas con áreas generales vinculadas a una especialidad médica o investigadora.

Se considerará lícita y compatible la reutilización de datos personales con fines de investigación en materia de salud y biomédica cuando, habiéndose obtenido el consentimiento para una finalidad concreta, se utilicen los datos para finalidades o áreas de investigación relacionadas con el área en la que se integrase científicamente el estudio inicial.

En los casos indicados en el párrafo anterior, los responsables deberán publicar la información establecida por el artículo 13 RGPD en un lugar fácilmente accesible de la página web corporativa del centro donde se realice la investigación o estudio clínico, y, en su caso, en la del promotor, y notificar la existencia de esta información por medios electrónicos a los afectados. Cuando estos carezcan de medios para acceder a tal información, podrán solicitar su remisión en otro formato.

Para los tratamientos de reutilización de datos personales con fines de investigación en materia de salud y biomédica, se requerirá informe previo favorable del comité de ética de la investigación.

Se considera lícito el uso de datos personales "seudonimizados" con fines de investigación en salud y, en particular, biomédica.

El uso de datos personales "seudonimizados" con fines de investigación en salud pública y biomédica requerirá:

a. El informe previo del comité de ética de la investigación previsto en la normativa sectorial. En defecto de la existencia del mencionado Comité, la entidad responsable de la investigación requerirá informe previo del delegado de protección de datos.

b. Una separación técnica y funcional entre el equipo investigador y quienes realicen la "seudonimización" y conserven la información que posibilite la reidentificación.

c. Que los datos "seudonimizados" únicamente sean accesibles al equipo de investigación cuando:

i. Exista un compromiso expreso de confidencialidad y de no realizar ninguna actividad de reidentificación.

ii. Se adopten medidas de seguridad específicas para evitar la reidentificación y el acceso de terceros no autorizados.

Podrá procederse a la reidentificación de los datos en su origen, cuando con motivo de una investigación que utilice datos "seudonimizados", se aprecie la existencia de un peligro real y concreto para la seguridad o salud de una persona o grupo de personas, o una amenaza grave para sus derechos o sea necesaria para garantizar una adecuada asistencia sanitaria.

Cuando se traten datos personales con fines de investigación en salud, y en particular la biomédica, a los efectos del artículo 89.2 RGPD, podrán **excepcionar los derechos de los afectados** previstos en los artículos 15, 16, 18 y 21 RGPD cuando:

a. Los citados derechos se ejerzan directamente ante los investigadores o centros de investigación que utilicen datos anonimizados o "seudonimizados".

b. El ejercicio de tales derechos se refiera a los resultados de la investigación.

c. La investigación tenga por objeto un interés público esencial relacionado con la seguridad del Esta- do, la defensa, la seguridad pública u otros objetivos importantes de interés público general, siempre que en este último caso la excepción esté expresamente recogida por una norma con rango de Ley.

Por último, cuando conforme a lo previsto por el artículo 89 RGPD, se lleve a cabo un tratamiento con fines de investigación en salud pública y, en particular, biomédica se procederá a:

a. Realizar una evaluación de impacto que determine los riesgos derivados del tratamiento en los supuestos previstos en el artículo 35 del RGPD o en los establecidos por la autoridad de control. Esta evaluación incluirá de modo específico los riesgos de reidentificación vinculados a la "anonimización" o "seudonimización" de los datos.

b. Someter la investigación científica a las normas de calidad y, en su caso, a las directrices internacionales sobre buena práctica clínica.

c. Adoptar, en su caso, medidas dirigidas a garantizar que los investigadores no acceden a datos de identificación de los interesados.

d. Designar un representante legal establecido en la Unión Europea, conforme al artículo 74 RGPD, si el promotor de un ensayo clínico no está establecido en la Unión Europea. Dicho representante legal podrá coincidir con el previsto en el artículo 27.1 RGPD."

Para mayor precisión procede remitir a otros documentos de referencia europeos, de la AEPD y de la misma autoridad catalana.[96]

[96] Dictámenes emitidos recientes por la Autoridad Catalana de Protección de Datos en los que se analiza el régimen establecido por la Disposición Adicional 17 Ley orgánica 3/2018, para el tratamiento de datos de salud en el marco de la investigación:

También se ha recordado que[97] **los datos de las historias clínicas de los pacientes**, por interpretación conjunta de la Ley 41/2002 y de la Disposición Adicional 17 de la LO 3/2018, se podrán utilizar para investigación de forma seudonimizada, siempre que se cumplan los requisitos de la LOPD-GDD (separación entre el equipo investigador y quien realiza la seudonimización, y exista un compromiso de confidencialidad y de no reutilización de los datos).

También la normativa admite llevar a cabo estudios científicos en materia de salud pública, sin el consentimiento de los afectados en **situaciones de excepcional relevancia y gravedad para la salud pública.**

Dictamen Autoridad Catalana de Protección de Datos CNS 15/2019. el tratamiento de datos seudonimizados con finalidades de investigación y base de legitimación

Dictamen Autoridad Catalana de Protección de Datos CNS 18/2019. analiza otros aspectos de la Disposición Adicional 17

Dictamen 3/2019, sobre "Preguntas y Respuestas sobre la interrelación entre la regulación de ensayos clínicos y el RGPD" de 23 de enero de 2019, del Comité Europeo de Protección de Datos.

Informe 073667/2018 AEPD https://www.aepd.es/informes/juridicos/

https://www.aepd.es/media/informes/2018-0046-investigacionbiomedica.Pdf

[97] Méndez García, Miriam y Alfonso Farnós, Iciar, "La legitimación para el tratamiento de categorías especiales de datos con finalidades de investigación en el marco del Reglamento (UE) 2016/679 y de la Ley Orgánica 3/2018", en *Revista de derecho y genoma humano: genética, biotecnología y medicina avanzada* Nº Extra 1, 2019 (Ejemplar dedicado a: Uso de datos clínicos ante nuevos escenarios tecnológicos y científicos. Oportunidades e implicaciones jurídicas), págs. 205-231, p. 229.

XI. ¿QUÉ OBLIGACIONES HAY QUE CUMPLIR SI SE TRATAN DATOS Y QUÉ MEDIDAS HAY QUE ADOPTAR?

1. "Más vale prevenir que curar". El modelo proactivo del RGPD

El nuevo Reglamento europeo de protección de datos apuesta por mecanismos proactivos y preventivos en vez de reactivos, en otras palabras, más vale prevenir que curar. El principio de responsabilidad proactiva incorpora una filosofía de acción que apuesta por el valor del diseño tecnológico basado en el cumplimiento normativo. El RGPD ha subrayado la obligación de actuación en defensa y prevención de riesgos a través de la llamada *accountability* o deber proactivo de adoptar medidas ordenadas a garantizar el cumplimiento normativo, procesos del diseño basado en privacidad o el desarrollo de metodologías de análisis de riesgos o *Privacy Impact Assessment*[98]. Así, impone la protección de datos desde el diseño y por defecto (art. 25)[99], de modo que la privacidad se

[98] Considerando 78: "el responsable del tratamiento debe adoptar políticas internas y aplicar medidas que cumplan en particular los principios de protección de datos desde el diseño y por defecto. Dichas medidas podrían consistir, entre otras, en reducir al máximo el tratamiento de datos personales, seudonimizar lo antes posible los datos personales, dar transparencia a las funciones y el tratamiento de datos personales, permitiendo a los interesados supervisar el tratamiento de datos y al responsable del tratamiento crear y mejorar elementos de seguridad. Al desarrollar, diseñar, seleccionar y usar aplicaciones, servicios y productos que están basados en el tratamiento de datos personales o que tratan datos personales para cumplir su función, ha de alentarse a los productores de los productos, servicios y aplicaciones a que tengan en cuenta el derecho a la protección de datos cuando desarrollan y diseñen estos productos, servicios y aplicaciones, y que se aseguren, con la debida atención al estado de la técnica, de que los responsables y los encargados del tratamiento están en condiciones de cumplir sus obligaciones en materia de protección de datos. Los principios de la protección de datos desde el diseño y por defecto también deben tenerse en cuenta en el contexto de los contratos públicos."

[99] "el responsable del tratamiento debe adoptar políticas internas y aplicar medidas que cumplan en particular los principios de protección de datos desde el diseño y por defecto. Dichas medidas podrían consistir, entre otras, en reducir al máximo el tratamiento de datos personales, seudonimizar lo antes posible los datos personales, dar transparencia a las funciones y el tratamiento de datos personales, permitiendo a los interesados supervisar el tratamiento de datos y al responsable del tratamiento crear y mejorar elementos de seguridad. Al desarrollar, diseñar, seleccionar y usar aplicaciones, servicios y productos que están basados en el tratamiento de datos personales o que tratan datos personales para cumplir su función, ha de alentarse a los productores de los productos, servicios y aplicaciones a que tengan en cuenta el derecho a la protección de datos cuando desarrollan y diseñen estos productos, servicios y aplicaciones, y que se aseguren, con la debida atención al estado de la técnica, de que los responsables y los encargados del tratamiento están en condiciones de cumplir sus obligaciones en materia de protección de datos. Los principios de la protección de datos desde el diseño y por defecto también deben tenerse en cuenta en el contexto de los contratos públicos.""

integre desde el inicio en el diseño, la gestión y ciclo de vida del tratamiento de datos. La protección de datos se ha de seguir desde el mismo desarrollo y diseño de productos.

En consecuencia, quienes traten datos como responsables o encargados, según el tipo de datos y tipo de tratamiento que realizan y sus riesgos deben elegir las medidas técnicas y organizativas de seguridad más eficaces para garantizar la seguridad de los datos tratados. Además, bajo la responsabilidad demostrada, han de poder demostrar el cumplimiento de los requisitos exigibles.

Este enfoque se basa en el necesario análisis y la gestión de riesgos para hacer un diagnóstico y adoptar las medidas técnicas y organizativas apropiadas atendiendo a la naturaleza, el ámbito, el contexto y la finalidad del tratamiento, así como considerando el riesgo. Procede (1) identificar, analizar y determinar cuáles son los riesgos; (2) la evaluación del riesgo y (3) tomar las medidas para reducir la probabilidad y el impacto.

Como se ha expuesto, en el ámbito de la investigación se flexibilizan no pocas obligaciones y requisitos en el tratamiento de datos. Y el modelo básico es que esta flexibilización se da *a cambio* de la efectiva disposición de garantías y adopción de técnicas (art. 89. 1º RGPD). Garantías como acuerdos de confidencialidad y cláusulas contractuales de compromiso de no reidentificación y mantenimiento de la anonimización auditorías de uso de la información anonimizada, etc.[100]

2. Obligaciones concretas que implica la responsabilidad proactiva

De modo más concreto, en el RGPD la responsabilidad proactiva implica:

- Art. 25 RGPD. **Protección de datos desde el diseño y por defecto** con anterioridad al inicio del tratamiento y también mientras se esté desarrollando, las medidas técnicas y organizativas adecuadas para ofrecer las garantías necesarias y garantizar el cumplimiento de los requerimientos del RGPD.
- Art. 28 RGPD. Cuando se precise un encargado del tratamiento hay que ser diligente en su elección para que ofrezca las garantías suficientes para aplicar **medidas técnicas y organizativas apropiadas**
- Art. 29 RGPD. Tratamiento bajo la autoridad del responsable o del encargado.
- Art. 30 RGPD. **Registro interno de las actividades del tratamiento** que realice la organización, todas deben ser revisadas y documentadas identificando el análisis del riesgo en cada tratamiento. El artículo 31 Ley Orgánica 3/2018, de 5 de diciembre, vincula el registro de actividades de tratamientos (en la línea de la anterior LOPD al concepto de “conjuntos estructurados de datos”, no tanto a

[100] Alkorta Idiakez Itziar, “Regulación del tratamiento de los datos en proyectos de investigación sanitaria, en especial, en la aplicación de las tecnologías Bigdata”, en *Revista de derecho y genoma humano: genética, biotecnología y medicina avanzada* Nº Extra 1, 2019 (Ejemplar dedicado a: Uso de datos clínicos ante nuevos escenarios tecnológicos y científicos. Oportunidades e implicaciones jurídicas), págs. 273-323, p. 289.

ficheros en particular. Igualmente prescribe que el responsable y el encargado que designen un delegado de protección de datos lo incluyan en el registro de actividades. También, para el sector público, el artículo 31 con el artículo 77.1 impone publicar un inventario de actividades de tratamiento, el mismo ha de expresar también la base que legitima el tratamiento de cada actividad.

- Art. 31 RGPD. Cooperación con la autoridad de control.
- Art. 32 RGPD. Decidir qué **medidas técnicas y organizativas** son las adecuadas según los riesgos que comporte el tratamiento.
- Art. 33 RGPD. **Notificación de una violación de la seguridad** de los datos personales a la autoridad de protección de datos.
- Art. 34 RGPD. **Comunicación de una violación de la seguridad** de los datos personales al interesado.
- Art. 35 RGPD. **Evaluación de impacto** relativo a la protección de datos. De especial importancia para el ecosistema del big data y la inteligencia artificial, el uso de decisiones algorítmicas y perfilados respecto de humanos obliga efectuar la evaluación de impacto de protección de datos (art. 35 RGPD-UE, AEPD mayo 2019), esto es, el análisis y descripción de todas las operaciones, su necesidad y la proporcionalidad y la evaluación de los riesgos (al respecto, G29-UE, 2018: 3 y ss.).
- Art. 36 RGPD. Designación del delegado de protección de datos.

Excede a este documento el detalle de cómo cumplir con las obligaciones. No obstante, hay documentos especialmente preparados para facilitar el cumplimiento. A este respecto cabe destacar:

Listado de elementos para el cumplimiento normativo

Guía para responsables del tratamiento

Guía práctica para las evaluaciones de impacto en la protección de datos personales

Guía cumplimiento RGPD

Estudio de impacto Guía eipd

Guía de Privacidad desde el Diseño [oct 2019]

Guía para clientes que contraten servicios de Cloud Computing [sep 2018]

Orientaciones para prestadores de servicios de Cloud Computing [sep 2018]

Guía para la gestión y notificación de brechas de seguridad

Guía práctica de análisis de riesgos para el tratamiento de datos personales [feb 2018]

3. Las variadas medidas técnicas y organizativas de seguridad

Las medidas técnicas y organizativas de seguridad son muy variadas, entre otras muchas, puede seguirse las mencionadas en el Reglamento UPV.

Medidas de seguridad

(marque lo que corresponda)

- Se ha realizado un análisis de riesgos
- Definición de funciones y obligaciones del personal
- Se ha formado al personal
- Se aplica un estándar ISO
- Sistemas de identificación y autenticación
- Declaración y gestión de incidentes de seguridad
- Se aplica el Esquema Nacional de Seguridad
- Trazabilidad (log de acceso y acciones de los usuarios)
- Protocolos de notificación de la violación de la seguridad de los datos
- Se aplica el RLOPD
- Copia de respaldo y recuperación (back-up) en los servidores propios y servidores en cloud
- Medidas en la sincronización de Protocolos de recuperación de datos
- Se han adoptado medidas de Seudoanonimización
- Cifrado Controles de acceso físico
- Protección del entorno de comunicaciones del sistema de información
- Seguridad en soportes no automatizados
- Auditoría de los sistemas de información
- Controles de acceso lógico
- Existe una persona responsable de la seguridad
- Existe un documento de seguridad
- Gestión de soportes y documentos (inventario de activos, entradas y salidas de datos etc.)
- Existen medidas de seguridad cuando se usan los datos fuera de los locales de la UPV
- Se adoptan medidas de seguridad cuando se crean, exportan y usan datos personales en ficheros de uso temporal
- Existen contratos con obligaciones de seguridad en servicios externalizados
- Otras (Indique cuáles)

Como se recuerda para la UNED[101], las medidas de seguridad tienen como finalidades principales garantizar la integridad de la información, permitir su recuperación en caso de incidentes y evitar los accesos no autorizados a las mismas. Por ello, el RGPD contempla medidas de seguridad que deben adaptarse a las características de los tratamientos, al tipo de datos tratados o a la tecnología disponible en cada momento.

[101] Código de conducta UNED, p. 28.

Para cada uno de los tratamientos se realizará su respectivo análisis de riesgo o evaluación de impacto de privacidad para determinar las medidas de seguridad a aplicar.

En todo caso se tendrán en cuenta:

A. El cifrado de datos personales en el tratamiento de categorías especiales de datos.
B. La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.
C. La capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico.
D. La coordinación de la gestión en materia de seguridad por el Comité de Seguridad de la Información. Para ello evalúa y valora la eficacia de las medidas técnicas y organizativas para garantizar la seguridad de los tratamientos.

4. Las quiebras de seguridad y el deber de su notificación y comunicación

El RGPD[102] define las violaciones de seguridad de los datos, más comúnmente conocidas como “quiebras de seguridad”, de una forma muy amplia, que incluye todo incidente que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos. Sucesos como la pérdida de un ordenador portátil, el acceso no autorizado a las bases de datos de una organización (incluso por su propio personal) o el borrado accidental de algunos registros constituyen violaciones de seguridad a la luz del RGPD y deben ser tratadas como el Reglamento establece.

Cuando se produzca una violación de la seguridad de los datos, el responsable debe notificarla a la autoridad de protección de datos competente, a menos que sea improbable que la violación suponga un riesgo para los derechos y libertades de los afectados.

La notificación de la quiebra a las autoridades debe producirse sin dilación indebida y, a ser posible, dentro de las 72 horas siguientes a que el responsable tenga constancia de ella.

La notificación ha de incluir un contenido mínimo:

- La naturaleza de la violación
- Categorías de datos y de interesados afectados
- Medidas adoptadas por el responsable para solventar la quiebra

[102] Código de conducta UNED, p. 28.

- Si procede, las medidas aplicadas para paliar los posibles efectos negativos sobre los interesados

Los responsables deben documentar todas las violaciones de seguridad.

En los casos en que sea probable que la violación de seguridad entrañe un alto riesgo para los derechos o libertades de los interesados, la notificación a la autoridad de supervisión deberá complementarse con una notificación dirigida a estos últimos.

El objetivo de la notificación a los afectados es permitir que puedan tomar medidas para protegerse de sus consecuencias. Por ello, el RGPD requiere que se realice sin dilación indebida, sin hacer referencia ni al momento en que se tenga constancia de ella ni tampoco a la posibilidad de efectuar la notificación dentro de un plazo de 72 horas. El propósito es siempre que el interesado afectado pueda reaccionar tan pronto como sea posible.

5. La formación e información como medida activa eficaz

La eficacia de la normativa no se logra con el mero cumplimiento formal de las obligaciones establecidas en el RGPD. La eficacia del Código se logrará cuando se alcance un alto nivel de concienciación por parte de los usuarios del Sistema de Información.

Para ello es del todo recomendable una labor proactiva en la formación, así como en la información y asesoramiento a los miembros y equipos de la organización. Es del todo recomendable que haya una planificación específica al respecto y órganos o unidades encargadas o responsables. La oferta formativa es variada y se ha de estimular la participación en reuniones, cursos y jornadas, asó como materiales didácticos eficaces como videos y videotutoriales.

Toda la planificación de actividad de formación debe estar alineada con la actividad y criterios del DPD de la organización, a quien hay que invitar a adoptar un papel protagonista en la organización.

XII. ESPECIAL ATENCIÓN A LA ANONIMIZACIÓN Y SEUDOANONIMIZACIÓN. UNA ESTRATEGIA BÁSICA PARA PODER TRATAR DATOS PARA LA INVESTIGACIÓN

1. La anonimización (agregación) como posible vía para eludir la normativa de protección de datos o, especialmente, como medida de seguridad exigible en particular en la investigación

Una clave jurídica esencial para que sea aplicable el régimen de protección de datos es si se da la premisa de que los variados macrodatos sean datos personales. **Si no son datos de personas concretas identificadas o identificables, o reidentificables, y no se aplica la legislación**. Así pues, será posible escapar del exigente régimen de protección de datos si se da una anonimización (agregación) y garantice que los datos no vuelvan a ser personales [103].

Para poder escapar a la aplicación normativa es preciso garantizar la irreversibilidad de la anonimización o agregación de los datos. Para ello han de valorarse las fuentes de información disponibles, la tecnología aplicable en los procesos de anonimización y en los de reidentificación. Ahora bien, dado que la anonimización no sería nunca absoluta, se trata de que el esfuerzo de reidentificación de los sujetos conlleve un coste suficientemente[104]. El avance de la tecnología y la información disponible hacen difícil garantizar el anonimato absoluto o, de hecho, no ser lo buscado. De ahí que como a continuación se explica, no se busque una anonimización completa. Así, por ejemplo, en ámbitos como la salud en los que puede ser necesario identificar a personas cuyos datos han servido a la investigación en razón de riesgos de salud.

> Hay que advertir que en cierto modo la actual visión de la AEPD (PS/00326/2018 de julio 2019) parece restrictiva y muy difícil escapar al régimen de protección de datos pese a una fuerte anonimización de los datos que se dio en aquel caso.

La anonimización interesa más allá de la posibilidad de eludir la normativa de protección de datos[105], sino **para gozar de las especiales ventajas del tratamiento de datos para la investigación.** Bajo el marco del artículo 89. 1º RGPD una vez más cabe recordar que se

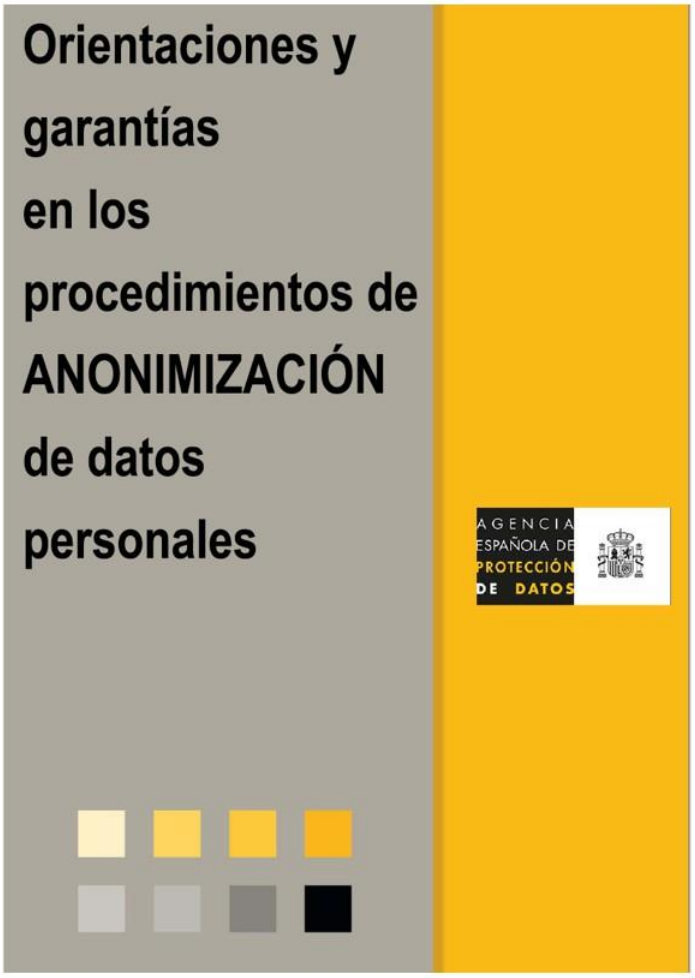
[103] Dictamen 05/2014, del Grupo de Trabajo del Artículo 29 (WP 216), relativo a técnicas de anonimización. También Guía Big Data AEPD-ISMS, 2017 pp. 40 y ss.

[104] AEPD Guía Orientaciones y garantías …p. 4.

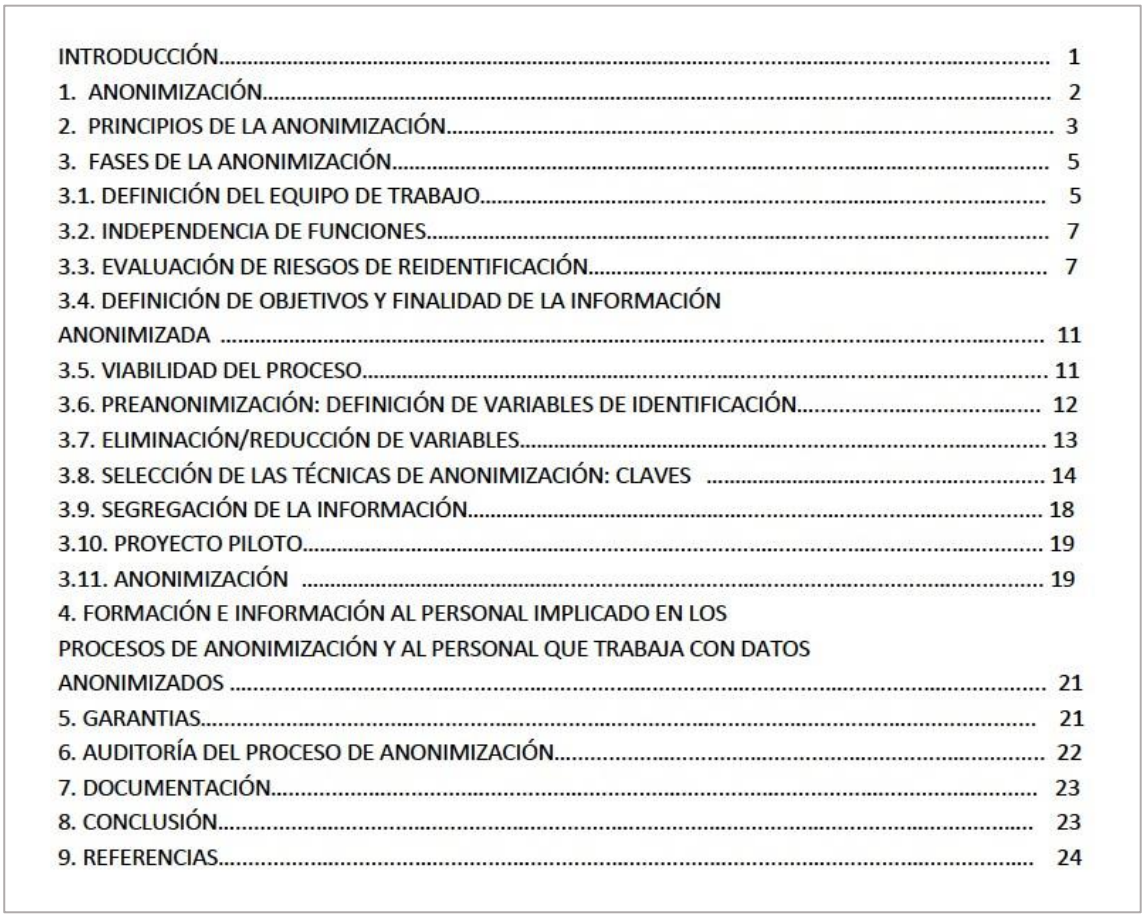
[105] AEPD Guía Orientaciones y garantías … pp. 1-2.

facilita el uso para la investigación *a cambio* de "garantías adecuadas" de minimización de los datos personales. Y especialmente las técnicas de seudonimización son esenciales.

En 2019 la AEPD ha prestado particular atención a la anonimización en su Nota técnica "La K-anonimidad como medida de la privacidad" y en su amplia Guía Orientaciones y garantías en los procedimientos de anonimización de datos personales



Guía AEPD sobre anonimización.



Índice de la Guía AEPD sobre anonimización.

Como se ha señalado con acierto[106], el Reglamento se ha rendido a la evidencia de que ante el progresivo aumento de la capacidad de procesamiento y de cruce de datos anonimizados es imposible en la actualidad, y menos en el futuro, seguir manteniendo la idea de que se pueden anonimizar los datos de forma irreversible dado que, al final, cualquier dato suficientemente enriquecido y combinado con otros, es susceptible de ser reidentificado.

2. Anonimización y seudoanonimización

Así, la anonimización y seudoanonimización es una de las garantías o mecanismos de seguridad para el manejo y tratamiento masivo de datos procedentes de los ciudadanos mediante el uso de técnicas basadas en Big Data, Inteligencia Artificial o Machine Learning.

[106] Alkorta Idiakez Itziar, "Regulación del tratamiento de los datos en proyectos de investigación sanitaria, en especial, en la aplicación de las tecnologías Bigdata", en *Revista de derecho y genoma humano: genética, biotecnología y medicina avanzada* Nº Extra 1, 2019 (Ejemplar dedicado a: Uso de datos clínicos ante nuevos escenarios tecnológicos y científicos. Oportunidades e implicaciones jurídicas), págs. 273-323, p. 289.

> Bajo el principio de accountability y responsabilidad proactiva, el responsable del tratamiento debe analizar los riesgos de reidentificación en sus procesos de anonimización. Por ello debe escoger el tipo de atributos cuasi-identificadores utilizados con el objetivo de reducir la probabilidad de que el cruce de dichos campos con otros contenidos en fuentes de datos externas pueda representar un riesgo para los sujetos afectados. [107]

El objetivo del proceso de anonimización es producir la ruptura de la cadena de identificación de las personas. Las fuentes de datos empleadas para los tratamientos contienen datos personales que se catalogan como *"identificadores"* que, por sí solos, están asociados de forma unívoca a un sujeto, como son el DNI, el nombre completo, el pasaporte o el número de la seguridad social. Esta cadena de identificación se compone de microdatos o datos de identificación directa y de datos de identificación indirecta[108]. Así pues, el proceso de **anonimización consiste en disociar de los identificadores el resto de los datos más genéricos asociados a un sujeto como la fecha de nacimiento, el municipio de residencia, el género, etc**. El conjunto de datos preservados serán aquellos necesarios para cumplir con el objetivo del tratamiento y, mediante la su conservación y enriquecimiento, explotarlo para extraer información adicional.

Por su parte, cabe tener en cuenta la **Seudoanonimización**, especialmente recogida como mecanismo de garantía y seguridad en el RGPD, a partir de conocer la dificultad de conseguir una anonimización perfecta o que garantice, en términos absolutos, el enmascaramiento de la identidad de las personas.[109]

> El art. 4 RGPD la define: "5) «seudonimización»: el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable;"

Figura 1: Anonimización[110]

Asimismo, cabe señalar que la **k-anonimidad** es una propiedad de los datos anonimizados que permite cuantificar hasta qué punto se preserva la anonimidad de los sujetos

[107] AEPD Guía Orientaciones y garantías …p. 8.

[108] datos cruzados de la misma o de diferentes fuentes que pueden permitir la reidentificación de las personas, como la información de otras bases de datos del mismo u otro responsable, de las redes sociales, buscadores, blogs, etc.

[109] AEPD, Nota técnica "La K-anonimidad … p. 2.

[110] AEPD, Nota técnica "La K-anonimidad … p. 3.

presentes en un conjunto de datos en el que se han eliminado los identificadores. Dicho de otro modo, es una medida del riesgo de que agentes externos puedan obtener información de carácter personal a partir de datos anonimizados.

3. Orientaciones y garantías en los procedimientos de anonimización de datos personales

La adopción de técnicas de **anonimización o seudoanonimización** pasan a formar parte de la **estrategia básica** del tratamiento de datos en una organización dedicada al tratamiento masivo de datos.

La propia **anonimización o seudoanonimización son en sí un tratamiento de datos**. Resulta conflictivo el hecho de que requieran un consentimiento del interesado para legitimar el tratamiento, como señala Casabona[111].

> A falta de una interpretación "oficial", cautelarmente si se obtiene el consentimiento del interesado inicialmente interesará informar de posteriores procesos de anonimización o seudoanonimización para su uso investigador.

En la estrategia en la organización, la AEPD subraya la **importancia de segregar y diferenciar funciones, papeles y responsables en la cadena y proceso de anonimización**[112], pues ello en sí es una garantía frente a la reidentificación. Se requiere también seguir el principio de independencia profesional de los equipos de trabajo.

Así la AEPD separa perfiles y atribuciones para (1) equipo de seguridad de la información[113]; (2) el responsable de protección de datos o, si existiera, DPD[114]; (3) quien

---

[111] Romeo Casabona Carlos María, "Revisión de las categorías jurídicas de la normativa europea ante la tecnología del big data aplicada a la salud", *Revista de derecho y genoma humano: genética, biotecnología y medicina avanzada* Nº Extra 1, 2019 (Ejemplar dedicado a: Uso de datos clínicos ante nuevos escenarios tecnológicos y científicos. Oportunidades e implicaciones jurídicas), págs. 85-128, p. 110.

[112] AEPD Guía Orientaciones y garantías …pp. 5-6.

[113] -equipo de seguridad de la información y del proceso de anonimización: responsable de seguridad y resto del personal involucrado en tareas de seguridad de la información (operadores de seguridad, responsables de seguridad de la información departamentales o de zona, responsables de sistemas de información, etc.), comité ético, etc.

[114] Debe hacer evaluaciones de impacto previo sobre la privacidad en los procesos de anonimización, verificar la ejecución de los procesos de anonimización, velar por la independencia de roles y funciones, reportar al responsable de la información y del tratamiento sobre los procesos de anonimización, promover auditorías de cumplimiento de los procesos de anonimización o atender las solicitudes de información de los ciudadanos con relación a sus datos personales anonimizados o no, entre otras funciones.

recibe los datos o información anonimizada y quienes deciden los objetivos finales a los que se destina la misma. También recomienda que haya un equipo de evaluación de riesgos inicial[115], equipo de preanonimización y anonimización encargado de elegir las técnicas de anonimización necesarias y de su aplicación y Equipo de seguridad de la información y del proceso[116].

También la AEPD detalla todas las fases del proceso[117]:

- Identificación y categorización de activos implicados en el proceso de anonimización[118].
- Constitución del equipo de trabajo.
- Identificación de riesgos de reidentificación existentes conocidos, potenciales y no conocidos.
- Salvaguardas.
- Cuantificar el impacto[119].
- Informe de riesgos:
  - Determinación del umbral de riesgos aceptable.
  - Gestión de los riesgos asumibles.

[115] Del proceso de anonimización, que audite el procedimiento de anonimización y el uso de la información anonimizada y responsable en última instancia de asegurar que el fichero anonimizado cumple con los requisitos valorar la fortaleza de los procedimientos que deben garantizar la irreversibilidad de la anonimización.

[116] vela por las medidas de seguridad que pudieran ser necesarias durante el ciclo de vida de la información anonimizada y durante los procesos de anonimización, además de valorar los resultados de la EIPD e implantar las medidas encaminadas a paliar los riesgos para la información personal anonimizada

[117] AEPD Guía Orientaciones y garantías …pp. 7 y ss.

[118] Detallando:

a. Datos personales a anonimizar.
b. Activos de información anonimizada y variables de identificación asociadas.
c. Procesos y subprocesos de anonimización.
d. Sistemas de información implicados: hardware utilizado, limitación del software de anonimización con relación a los activos de información que sea preciso anonimizar.
e. Análisis de dependencias de activos implicados en el proceso de anonimización.
f. Categorización de los activos: es posible establecer una categorización en función de la criticidad de cada activo, teniendo en cuenta aspectos como, por ejemplo, grado de sensibilidad de la información.

[119] Impacto puede ser tangible (por ejemplo, daños materiales, posibles indemnizaciones, etc.) o intangible (pérdida de confianza, deterioro de la imagen del responsable del tratamiento, estigmatización de los interesados, etc.),

- Informe final.
- Revisión de riesgos periódicas.

Asimismo, determinados los papeles, personal y atribuciones se llevan a cabo

1º "Preanonimización" [120] esto es, la categorización de las variables y su clasificación y sensibilidad para pasar a la *eliminación/reducción de variables*, esto es, reducir al mínimo necesario la cantidad de variables que permitan la identificación de las personas.

2º Luego se lleva a cabo la *selección de las técnicas de anonimización: claves algoritmos de hash*[121]. Las técnicas a emplear son variables:

- mecanismo criptográfico[122]
- algoritmo de cifrado homomórfico[123]
- anonimización por capas[124]
- perturbación de datos[125]
- reducción de datos sin alterar los mismos
- segregación de la información[126]

[120] AEPD Guía Orientaciones y garantías …pp. 15 y ss.

[121] AEPD Guía Orientaciones y garantías … p. 13.

[122] Se ha de utilizar un mecanismo criptográfico que nos garantice el secreto de la huella digital que hemos generado.

[123] Por su parte un algoritmo de cifrado homomórfico permite realizar operaciones con datos cifrados de tal manera que el resultado de las operaciones es el mismo que si las operaciones se hubieran realizado con los datos sin cifrar.

[124] También pueden utilizarse las la anonimización por capas, de forma que existan varios niveles de anonimización. Así, según el nivel de criticidad se aplican distintas claves y proceder a una segunda o ulterior aplicación claves secretas. Estas técnicas de anonimización por capas pueden hacerse depender no del nivel de seguridad de la información, sino según la organización interna y el nivel de acceso de cada departamento. Así, se garantiza la privacidad de los datos anonimizados de forma interdepartamental.

[125] También se pueden seguir, Guía AEPD anonimización pp. 17 y ss. técnicas de *perturbación de datos*: Microagregación; Intercambio aleatorio de datos; Datos sintéticos (Distorsión de datos, Distorsión con microdatos híbridos), Permutación de registros, Permutación temporal, Redondeo, Reajuste, Ruido aleatorio

[126] Ibíd. p. 18. que garantice entornos separados para cada tratamiento de datos anonimizados, separando la explotación de la anonimización de la información. Igualmente la segregación del personal que accede a la información y a los datos personales.

3º Se debe realizar un proyecto piloto con una pequeña muestra de datos de prueba (no reales).

4º Finalmente, en la fase de anonimización se realiza la disociación definitiva e irreversible de los datos personales. En esta fase de anonimización pueden realizarse las siguientes **tareas o actividades**:

- Determinar la técnica de anonimización que sea más apropiada en función de las variables que hubieran sido identificadas en la fase de preanonimización.
- Planificación y asignación de tareas específicas a cada miembro del equipo de trabajo con relación a las funciones asignadas para cada perfil implicado en el proceso de anonimización.
- Determinar los recursos y equipo técnico necesarios para proceder a la anonimización de los datos.
- Validar la técnica de anonimización por expertos (unidad u organismo experto en estadística, ética, etc.)
- Aplicar la técnica seleccionada y ejecutar el proceso de anonimización; realizar pruebas.
- Ruptura relacional de las claves en función del uso de la información (uso interno y uso externo). Siempre que sea posible se utilizarán distintas claves en función del uso que vaya a darse a la información anonimizada.
- Recodificación o reducción de variables para los datos sensibles residuales tras el proceso de anonimización.
- Aplicar técnicas de reducción de datos (supresión de campos que no sean significativos para el uso posterior).
- Acotar el nivel de desagregación en función del nivel geográfico afectado por el fichero y la sensibilidad de la información.
- Aplicar técnicas de perturbación de los datos (modificar datos cuantitativos en pequeñas cantidades aleatorias, intercambiar atributos de forma controlada entre registros de zonas geográficas próximas, respetando las distribuciones).
- Validación y aprobación de los archivos anonimizados por expertos y por el equipo de evaluación.
- Revisión periódica del proceso.
- Auditar el proceso de anonimización y el uso posterior de los datos mediante métricas o escalas que proporcionen una interpretación objetiva de los resultados.

La **anonimización requiere de *garantías*** como las que señala la AEPD[127]: Acuerdos de confidencialidad[128]; compromiso del destinatario de la información para mantener la anonimización y la obligación de informar al responsable del tratamiento ante cualquier sospecha de reidentificación y la realización de auditorías de uso de la información anonimizada por parte del responsable del tratamiento al responsable del tratamiento de los datos anonimizados.

Finalmente, todo ello queda inmerso en el modelo de responsabilidad demostrada, esto es, la anonimización correcta ***debe poder probarse a través de la documentación***[129]**.**

[127] AEPD Guía Orientaciones y garantías …pp. 22 y ss.

[128] De Responsable del tratamiento, del proceso de anonimización. del tratamiento de datos anonimizados; del personal con acceso a la información anonimizada

[129] Política de uso y acceso a los datos anonimizados: obligaciones del personal.

Documento de aplicabilidad de medidas de anonimización que contendrá al menos: Responsables del proceso de preanonimización y anonimización.

Medidas organizativas.

Definición de variables de identificación.

Mecanismos técnicos de anonimización.

Política de claves

Acuerdos de confidencialidad.

Normas y procedimientos.

Informes y dictámenes: Del equipo de viabilidad, del equipo de seguridad, de análisis de riesgos (EIPD) y de auditoría de la información y el proceso de anonimización.

XIII. ¿PUEDO ENVIAR LOS DATOS FUERA DE ESPAÑA?

Sin perjuicio de lo afirmado de los requisitos para comunicar datos, así como del acceso a los datos por corresponsables y encargados, hay **requisitos específicos para que los datos puedan moverse internacionalmente**.

Los datos personales que se manejen, en principio pueden transferirse dentro de la UE y del llamado Espacio Económico Europeo[130].

Sin embargo, en principio no pueden transferirse a otros países (terceros países, salvo que se den unos requisitos (artículos 45, 47 y 49 RGPD)[131].

- Sí que pueden transferirse a países respecto de los que la Comisión ha adoptado una decisión reconociendo que ofrecen un nivel de protección adecuado (Argentina, Guernsey, Isla de Man, Jersey, Islas Feroe, Andorra, Israel, Uruguay, Nueva Zelanda, Japón y Estados Unidos, Japón[132].

---

[130] Que incluye también (Liechtenstein, Islandia y Noruega

[131] Una información general sobre transferencias internacionales de la AEPD en https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/transferencias-internacionales

[132] Suiza. Decisión 2000/518/CE de la Comisión, de 26 de julio de 2000

Canadá. Decisión 2002/2/CE de la Comisión, de 20 de diciembre de 2001, respecto de las entidades sujetas al ámbito de aplicación de la ley canadiense de protección de datos

Argentina. Decisión 2003/490/CE de la Comisión, de 3 de junio de 2003

Guernsey. Decisión 2003/821/CE de la Comisión, de 21 de noviembre de 2003

Isla de Man. Decisión 2004/411/CE de la Comisión, de 28 de abril de 2004

Jersey. Decisión 2008/393/CE de la Comisión, de 8 de mayo 2008

Islas Feroe. Decisión 2010/146/UE de la Comisión, de 5 de marzo de 2010

Andorra. Decisión 2010/625/UE de la Comisión, de 19 de octubre de 2010

Israel. Decisión 2011/61/UE de la Comisión, de 31 de enero de 2011

Uruguay. Decisión 2012/484/UE, de la Comisión de 21 de agosto de 2012.

Nueva Zelanda. Decisión 2013/65/UE de la Comisión, de 19 de diciembre de 2012

Estados Unidos. Aplicable a las entidades certificadas en el marco del Escudo de Privacidad UE-EE.UU. Decisión (UE) 2016/1250 de la Comisión, de 12 de julio de 2016.

En todo caso, el **sistema con Estados Unidos** es algo más complejo y procede estar mejor informado[133]. En dos ocasiones el Tribunal de Justicia de la Unión Europea ha anulado el sistema especial para las transferencias de datos con aquél país ("Safe Harbour" y "Privacy Shield" en 2020). Resulta de especial interés seguir las Recomendaciones del Comité Europeo de Protección de Datos[134]

También pueden transferirse internacionalmente datos si se cuenta con unas garantías adecuadas sobre la protección que los datos recibirán en su destino. Para ello es de especial interés tener en cuenta las Cláusulas tipo de protección de datos adoptadas por una autoridad de control y aprobadas por la Comisión; los Códigos de conducta junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas las relativas a los derechos de los interesados o la existencia de Mecanismos de certificación. Resulta de especial interés seguir las "cláusulas contractuales estándar para la transferencia de datos personales a terceros países de conformidad con el Reglamento (UE) 2016/679" adoptadas por Decisión de Ejecución de la Comisión Europea en junio de 2021.

Si no se está en los casos anteriores, también es posible transferir datos si se dan una serie de requisitos, entre los que hay que destacar el **consentimiento del interesado**[135].

Si no se da alguna de los supuestos anteriores, se requiere **autorización** previa del Director de la Agencia Española de Protección de Datos.

Japón. Decisión de 23 de enero de 2019.

[133] Para ello cabe seguir las Preguntas más frecuentes en relación con la sentencia de la AEPD.

[134] Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, Adopted on 10 November 2020.

[135] a) El interesado haya dado explícitamente su consentimiento
b) La transferencia sea necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento o para la ejecución de medidas precontractuales adoptadas a solicitud del interesado
c) La transferencia sea necesaria para la celebración o ejecución de un contrato, en interés del interesado, entre el responsable del tratamiento y otra persona física o jurídica
d) La transferencia sea necesaria por razones importantes de interés público
e) La transferencia sea necesaria para la formulación, el ejercicio o la defensa de reclamaciones
f) La transferencia sea necesaria para proteger los intereses vitales del interesado o de otras personas, cuando el interesado esté física o jurídicamente incapacitado para dar su consentimiento
g) La transferencia se realice desde un registro público que, con arreglo al Derecho de la Unión o de los Estados miembros, tenga por objeto facilitar información al público y esté abierto a la consulta del público en general o de cualquier persona que pueda acreditar un interés legítimo, pero sólo en la medida en que se cumplan, en cada caso particular, las condiciones que establece el Derecho de la Unión o de los Estados miembros para la consulta.

Así pues, si se prevé la cooperación o contratación con organizaciones de fuera de la UE (o del EEE) es de interés tener en cuenta el tipo de país de que se trata. En el caso de datos tratados a través del consentimiento cautelarmente interesa contar con el consentimiento para la transferencia internacional de datos por los interesados para finalidades de investigación, etc.

De particular interés es el **uso de sistemas de nube**[136] ubicados fuera de la UE, particularmente en EEUU. Igualmente, en el ámbito académico y de investigación hay que tener especiales cautelas en el ámbito de títulos, certificaciones y la propia investigación con organismos extranjeros.

[136] Sobre el tema son de interés las Guías de la AEPD, así como Cotino Hueso, Lorenzo, "Algunas cuestiones clave de protección de datos en la nube. Hacia una 'regulación nebulosa'", en *Revista Catalana de Derecho Público* nº 51 (diciembre 2015), pp. 85-103 DOI: 10.2436/20.8030.01.55. Acceso texto completo http://revistes.eapc.gencat.cat/index.php/rcdp/article/view/10.2436-20.8030.01.55/n51-cotino-es.pdf

XIV. ¿PUEDEN LAS PERSONAS EJERCER DERECHOS Y RECLAMACIONES ANTE LAS ENTIDADES DE UN ECOSISTEMA DE INVESTIGACIÓN I-SPACES COMO DATA SPACE?

1. ¿Qué derechos pueden exigir los interesados?

La regulación de protección de datos reconoce diversos derechos a los interesados cuyos datos se tratan (derechos de acceso, rectificación, supresión -derecho al olvido-, oposición, portabilidad y limitación del tratamiento).

De modo muy sucinto cabe recordar:

-el derecho de acceso como el derecho del interesado a solicitar y obtener del responsable del tratamiento, gratuitamente, **información sobre el tratamiento** de sus datos de carácter personal (artículo 15 RGPD)

-derecho de **rectificación** como el derecho que tiene el interesado a rectificar sus datos cuando sean inexactos (artículo 16 RGPD).

- El responsable del tratamiento tendrá la obligación de **borrar** los datos cuando no sean ya necesarios, o ya no se tenga el consentimiento o la base de legitimación, cuando se trataron ilegalmente, cuando el interesado se oponga) (artículo 17 del RGPD).

-En los casos en los que se tratan datos sin el consentimiento del interesado, éste puede **oponerse** en cualquier momento y señalar los motivos relacionados con su situación particular para que dejen de tratarse (artículo 21 del RGPD,) a que los datos personales que le conciernan sean objeto de un tratamiento

-Uno de los nuevos derechos es el derecho a la **portabilidad** de los datos. Se trata del "derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado" (art. 20. 1º RGPD). Este derecho se aplicará cuando el tratamiento esté basado en el consentimiento o en la ejecución de un contrato y el tratamiento se efectúe por medios automatizados (art. 20. 1º RGPD).[137]

[137] Hay que tener presente las FAQ del Grupo del artículo 29 al respecto (http://apdcat.gencat.cat/web/.content/03-documentacio/Reglament_general_de_proteccio_de_dades/3122.pdf) y lo afirmado por la Agencia siguiendo aquéllas.

Otro de los nuevos derechos del RGPD es la **limitación de tratamiento** (art. 18 RGPD). Se trata del derecho a que cuando se solicite, los "datos solo podrán ser objeto de tratamiento, con excepción de su conservación, con el consentimiento del interesado o para la formulación, el ejercicio o la defensa de reclamaciones, o con miras a la protección de los derechos de otra persona física o jurídica o por razones de interés público importante de la Unión o de un determinado Estado miembro.protección de los derechos de otra persona física o jurídica o por razones de interés público importante de la Unión o de un determinado Estado miembro.

Más adelante con especial relación con la inteligencia artificial se hace referencia al **nuevo derecho respecto de decisiones automatizadas** (art. 22 RGPD).

Por cuanto al ámbito de la salud, especialmente hay que tener en cuenta recientes y excelentes documentos de la AEPD de los derechos de los usuarios de los servicios de salud[138] o más recientemente de la autoridad catalana[139].

2. ¿Qué obligaciones implican para quienes tratan datos personales?

Si las organizaciones o entidades de investigación tratan datos de interesados como responsables –o como encargados-, es una obligación poder dar respuesta al ejercicio de los derechos. Obviamente para ello se requerirá la condición de datos personales y la identificabilidad. Si la entidad que investiga no tiene capacidad de hacer los datos identificables porque se hayan separado funcionalmente en principio no será responsable de dar respuesta al ejercicio de derechos. Y lo cierto es que **estos derechos afectan y mucho a la gestión interna de toda organización que trate datos y obligan a tomar decisiones de organización de la información que quede dispuesta a posibilitarlos.**

Es imposible hacer efectivo el acceso si no se gestiona bien la información. De hecho, la posibilidad de ejercer estos derechos expresa un funcionamiento inadecuado de los procedimientos y gestión (por ejemplo, por no haber cancelado datos).

En el caso de la portabilidad, obliga a adoptar decisiones materiales de infraestructura tecnológica y de gestión.

Además, como se recuerda en el Considerando 59 "Deben arbitrarse fórmulas para facilitar al interesado el ejercicio de sus derechos […] El responsable del tratamiento

[138] AEPD, *Guía para pacientes y usuarios de la Sanidad*, noviembre 2019. Acceso en https://www.aepd.es/es/media/guias/guia-pacientes-usuarios-sanidad.pdf

[139] APDCAT, *Guía de protección de datos para pacientes y personas usuarias de los servicios de salud*, Autoritat Catalana de Protección de Datos, junio 2020. Acceso en https://apdcat.gencat.cat/es/documentacio/guies_basiques/Guies-apdcat/Guia-proteccio-de-dades-per-a-pacients/

también debe proporcionar medios para que las solicitudes se presenten por medios electrónicos". El artículo 13 no impone una obligación general de ejercicio electrónico de derecho (sólo "si procede"). Pero hay que estar a la regulación concreta de cada derecho y al desarrollo nacional.

De particular importancia en la gestión son derechos como la limitación del tratamiento y en especial la portabilidad.

Es bien posible que alguien pregunte la información que se tiene sobre él, y al conocerla pretenda que se rectifique o se suprima, o se oponga al tratamiento lícito de esta información, o quiera llevársela a otra parte. No obstante, pese a que estos derechos son afines, e incluso su ejercicio natural esté encadenado, se trata de derechos autónomos o independientes.

Estos derechos quedan desarrollados y regulados en el RGPD. Por cuanto a su régimen general cabe tener en cuenta que:

- El ejercicio es gratuito, no obstante, si las solicitudes son manifiestamente infundadas o excesivas (carácter repetitivo) el responsable podrá cobrar un canon proporcional a los costes administrativos soportados o negarse a actuar.

- Debe darse respuesta en el plazo general de un mes. No obstante, se puede prorrogar otros dos meses más, teniendo en cuenta la complejidad y número de solicitudes. Si el responsable no da curso a la solicitud, informará y a más tardar en un mes, de las razones de su no actuación y la posibilidad de reclamar ante una Autoridad de Control.

- El responsable está obligado a informar sobre los medios para ejercitar estos derechos. Estos medios deben ser accesibles y no se puede denegar este derecho por el solo motivo de que optes por otro medio. Así pues, hay elección de medio por afectado, no se le puede imponer un procedimiento determinado como el uso de un concreto impreso (art. 12 LOPD). No obstante, cabría darse la posibilidad de que el medio elegido diferente al electrónico podría generar costes que se trasladasen a afectado.

-Es muy importante para el responsable –o en su caso el encargado- genere un sistema de prueba, puesto que la "prueba del cumplimiento del deber de responder a la solicitud de ejercicio de sus derechos formulado por el afectado recaerá sobre el responsable" (art. 12. 4º LOPD)

- Son derechos personalísimos que se ejercen por el titular. Ahora bien, se pueden ejercer directamente o por medio de tu representante legal o voluntario. Si el responsable tiene dudas sobre la identidad, puede solicitar información adicional para confirmar la misma como la fotocopia del DNI o pasaporte u otro documento válido. También se puede usar la firma electrónica en vez del DNI. En el caso de representantes, la representación conferida o el documento o instrumento electrónico que acredite la representación.

El derecho puede denegarse por no poder verificar razonablemente la identidad del solicitante. Hay especialidades respecto de menores e incapaces[140]

La petición va dirigida al **responsable** que posea o trate los datos personales, a través de los mecanismos sobre los que está obligado a informar. Cabe la posibilidad de que, por cuenta del responsable, sea el **encargado** el que atienda tu solicitud, si ambos lo han establecido en el contrato o acto jurídico que les vincule (art. 12 LOPD)

La **comunicación para el ejercicio de derechos** incluirá, además de la identificación oportuna: la petición en que se concreta la solicitud; la dirección a efectos de notificaciones, fecha y tu firma y documentos acreditativos de la petición que realices, si fuesen necesario.

En la **respuesta** a quien ejerza el derecho es obligatorio informar sobre la posibilidad de invocar la tutela de la autoridad de control en caso de denegación que ahora, además, debe incluir la información sobre la posibilidad de acceso a la jurisdicción. Cabe señalar asimismo que ante el procedimiento del artículo 37 LOPD de reclamación voluntaria al DPD previa a la AGPD, debe informarse de esta posibilidad de acudir al DPD.

Para el caso de recibir cualquier petición o ejercicio de derechos procede sin duda comunicarlo al DPD

Por cuanto al ejercicio de los derechos en el ámbito de salud, la AEPD recuerda en general que los usuarios o pacientes tienen derecho a dirigirse al responsable del tratamiento de sus datos (médicos, centros de salud, centros sanitarios, tanto públicos como privados) solicitando el acceso a la documentación que constituye su historia clínica[141]. Y, como se ha adelantado, el acceso abarca la documentación electrónica y en papel. Ya se ha adelantado la importancia de generalizar el acceso avanzado por los interesados a la historia clínica electrónica. No obstante, como también se ha señalado ya respecto del MIOT y los datos desestructurados, las barreras de acceso efectivo y funcional son muchas.

[140] En los casos de incapacidad o minoría de edad se habrá de acreditar la condición de representante legal. En principio el menor que tenga la edad para consentir el tratamiento de datos (14 años) ejercerá por sí los derechos y los titulares de la patria potestad ejercerán los derechos de los menores de 14 años (art. 12 LOPD). Ahora bien, se trata de una cuestión compleja que puede llevar a que los padres o tutores tengan interés legítimo para solicitar información y datos por sus deberes y obligaciones (patria potestad, alimentos, etc.) y, por ello, puedan solicitar y acceder a información del menor mayor de 14 años, e incluso del mayor de edad.

[141] AEPD, Guía para pacientes y usuarios de la Sanidad, cit.

3. ¿Cuándo no es obligatorio dar respuesta a estos derechos, especialmente en la investigación?

Estos derechos serán exigibles salvo que hubiera una excepción legal (art. 23 RGPD). En todo caso, **hay que señalar que estas excepciones a los derechos pueden darse en el ámbito de la investigación** (art. 89 RGPD). Así, por ejemplo, no procede la información y transparencia obligatoria (art. 14.5º b) RGPD) cuando ello "resulte imposible o suponga un esfuerzo desproporcionado". El art. 89 2º RGPD excepciona diversos derechos "siempre que sea probable que esos derechos imposibiliten u obstaculicen gravemente el logro de los fines científicos y cuanto esas excepciones sean necesarias para alcanzar esos fines de investigación. Ello se proyecta respecto de los derechos reconocidos en los artículos 15, 16, 18, 19, 20 y 21. Además se regula específicamente respecto de la obligación de información (art. 14.5º b) RGPD), del derecho de supresión (art. 17. 3 d) RGPD) y el derecho de oposición (art. 21. 6º RGPD).

Para el caso de considerar que no procede reconocer el derecho cuando se ejerce, cabrá justificar bien por qué se considera que ello puede afectar a la finalidad de la investigación.

4. ¿Cuándo suprimo, borro y bloqueo datos? ¿A quién debo comunicarlo?

Por cuanto, a la supresión, debe señalarse que se trata de una **cuestión bien compleja la procedencia de la supresión de los datos y su efectivo borrado o "destrucción"** (art. 32 LOPD). Cuando proceda la supresión de los datos –también respecto de los datos rectificados- debe darse el "bloqueo" de los datos, esto es, "la identificación y reserva de los mismos, adoptando medidas técnicas y organizativas, para impedir su tratamiento, incluyendo su visualización".

Así pues, **los datos se mantienen, pero bloqueados (y con especiales medidas de seguridad)** y quedan fuera del flujo de datos de la organización y únicamente, sólo, "para

la puesta a disposición de los datos a los jueces y tribunales, el Ministerio Fiscal o las Administraciones Públicas competentes, en particular de las autoridades de protección de datos, para la exigencia de posibles responsabilidades derivadas del tratamiento y sólo por el plazo de prescripción de las mismas." Así pues, cuando procede suprimir los datos, no se borran o destruyen, sino que se mantienen bloqueados para atender posibles responsabilidades jurídicas de cada tipo de relación contractual, de consumo, administrativa, etc. Así, durante el plazo de prescripción de posibles responsabilidades, una vez pasado este plazo, procederá la destrucción.

Por cuanto al bloqueo el artículo 32.4º LOPD añade que cuando "la configuración del sistema de información no permita el bloqueo o se requiera una adaptación que **implique un esfuerzo desproporcionado**, se procederá a un copiado seguro de la información de modo que conste evidencia digital, o de otra naturaleza, que permita acreditar la autenticidad de la misma, la fecha del bloqueo y la no manipulación de los datos durante el mismo."

Asimismo, el apartado 5º remite a las autoridades de datos para establecer posibles "**excepciones a la obligación de bloqueo** […cuando éste] pudiera generar un riesgo elevado […o] un coste desproporcionado". Cabe añadir que como excepción no se dará el bloqueo respecto de la videovigilancia (art. 22 LOPD) y de los sistemas de denuncias internas (art. 24 LOPD).

Debe recordarse que el derecho a suprimir datos es diferente del derecho de los interesados a revocar o retirar su consentimiento.

En el caso de la supresión, es importante la regulación del artículo 17. 2º RGPD, por cuanto **si procede la supresión hay que informar a otros que traten datos de que se han suprimido**: "teniendo en cuenta la tecnología disponible y el coste de su aplicación, adoptará medidas razonables, incluidas medidas técnicas, con miras a informar a los responsables que estén tratando los datos personales de la solicitud del interesado de supresión de cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos."

De hecho, hay que tener en cuenta el artículo 19 para rectificación, supresión y limitación de tratamiento:

"El responsable del tratamiento comunicará cualquier rectificación o supresión de datos personales o limitación del tratamiento efectuada con arreglo al artículo 16 [rectificación], al artículo 17, apartado 1 [supresión], y al artículo 18 [limitación] a cada uno de los destinatarios a los que se hayan comunicado los datos personales, salvo que sea imposible o exija un esfuerzo desproporcionado. El responsable informará al interesado acerca de dichos destinatarios, si este así lo solicita."

Se trata de una novedad del RGPD relevante que habrá que implantar prácticamente y en cada supuesto y que puede implicar importantes acciones para quienes traten datos, especialmente en el ámbito de plataformas y prestadores de servicios de la sociedad de la información.

Un derecho que adquiere una potencial importancia en el ecosistema inteligencia artificial es el relativo a las decisiones automatizadas. Es bien posible que las tecnologías impliquen perfiles y decisiones sólo automatizadas relevantes para la persona, por lo que

será de aplicación el artículo 22 RGPD. Es por ello que cabe remitir a las garantías específicas que este "derecho" implica para, detalladas por el G29[142] o la AEPD: explicabilidad, transparencia, intervención humana, impugnación, posible estudio de impacto, mayor impacto en derechos y mayor responsabilidad proactiva, etc. No obstante, como punto de partida, las decisiones totalmente automatizadas en el ámbito de la investigación y en salud en principio no son frecuentes, por lo que no aplicaría específicamente el artículo 22 RGPD. Ahora bien, cabe recordar que el hecho de que las decisiones no sean plenamente automatizadas y relevantes supondrá que no apliquen estas especiales garantías, pero en modo excluye que rija el régimen de protección de datos y sus garantías si es que hay un tratamiento.

[142] Por todos, G29-UE. (2018). *Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679*, 3 de octubre de 2017, versión final 6 de febrero de 2018, Doc WP251rev.01. Acceso en https://www.aepd.es/sites/default/files/2019-12/wp251rev01-es.pdf

XV. ¿HAY DERECHOS O "PROPIEDAD" SOBRE LOS DATOS, EL BIG DATA O LOS ALGORITMOS?

Afirma con razón la Comisión Europea que "Los datos se han convertido en un activo clave para la economía y nuestras sociedades similares a las categorías clásicas de recursos humanos y financieros"[143]. Y ello se traduce en que no cabe duda de que los datos y el big data que manejan los miembros de organizaciones del Data Space - entidades que integran o agregan datos, así como los algoritmos que en su caso desarrollan son un activo, quizá el esencial. Al mismo tiempo, y del reverso la cuestión es si los miembros que forman parte del Data Space o entidades integradoras o agregadoras de datos (i-Spaces) pueden utilizar datos o algoritmo ajenos. Pues bien, lo cierto es que no está nada claro el marco jurídico de protección de dicho activo, ni el esquema regulatorio. La reciente propuesta de regulación de Reglamento de inteligencia artificial de la UE no regula la cuestión y únicamente puede seguirse una Resolución sobre propiedad intelectual e IA[144] del Parlamento Europeo.

Aunque la cuestión excede con mucho esta guía, cabe seguir algunas líneas al respecto[145], eso sí, hay que señalar que no se trata de una cuestión resuelta jurídicamente con la seguridad que requiere el sector.

Por cuanto a la protección del algoritmo parece que está descartada su patentabilidad[146], esto es, la protección por propiedad industrial.

---

[143] Digital Single Market. Policy on Big data, abril 2018. https://ec.europa.eu/digital-single-market/en/big-data

[144] Resolución del Parlamento Europeo, de 20 de octubre de 2020, sobre los derechos de propiedad intelectual para el desarrollo de las tecnologías relativas a la inteligencia artificial (2020/2015(INI)), https://www.europarl.europa.eu/doceo/document/TA-9-2020-0277_ES.html

[145] Se sigue, Ortega Giménez, Alfonso, "Implicaciones jurídicas de la internalización de la tecnología del Big Data y Derecho Internacional Privado", p. 169-204, en concreto pp. 180-186. De modo similar, Miralles Miravet Sergio, Big Data, un nou bé jurídic? En *Món jurídic: butlletí del Col.legi d'Advocats de Barcelona*, , Nº. 293, 2015, págs. 18-19, p. 19. Ver también González Royo, I., "La protección de los intangibles intelectuales e industriales en el contexto del Fintech", Diario La Ley, Núm. 8795, 2016. También, González Royo, I., y Pina, C. "¿Cómo se protegen legalmente los algoritmos?", en *Diario La Ley*, núm. 8776, 2016, p. 1. García Mirete, Carmen María, "Las bases de datos: intersección entre la propiedad intelectual y el derecho de la competencia europeo", en Nuevas fronteras del derecho de la Unión Europea", (coord. por Carlos Esplugues), 2012, , págs. 801-814

De interés, Aparicio Vaquero, Juan Pablo, "El valor económico de un derecho fundamental: la monetización de los datos personales", en *El Derecho de las TIC en Iberoamérica*, Obra Colectiva de FIADI (Federación Iberoamericana de Asociaciones de Derecho e Informática), La Ley- Thompson-Reuters, Montevideo, 2019, págs. 127-135.

[146] Como recuerda Ortega en el ámbito nacional, está descartado su patentabilidad debido a su consideración como mero método matemático por el artículo 4.4 de la Ley 24/2015 de

Recuerda Ortega, respecto al ámbito europeo, que se rechaza su patentabilidad por los mismos motivos en el artículo 52 del Convenio de Múnich (del que forma parte España desde 10 de julio de 1986). Se dispone que no serán patentables como invenciones "los descubrimientos, las teorías científicas y los métodos matemáticos" (art. 52.2.a). Tampoco "los planes, principios y métodos para el ejercicio de actividades intelectuales" (art. 52.2.c). La cámara de recursos de la Oficina Europea de Patentes ha rechazado varías solicitudes de patente de algoritmos. Y ello tiene claro reflejo en la normativa española que descarta la patentabilidad debido a su consideración como mero método matemático por el artículo 4.4 de la Ley 24/2015 de Patentes (letras a) y c). Y como consecuencia de la exclusión, tampoco pueden ser patentables como modelos de autoridad (art. 137. 2º Ley 24/2015).

Los algoritmos no tienen tampoco encaje como software protegible por la propiedad intelectual. Se trata también de un tema complejo. La Directiva 2009/24/CE afirma que la protección del software no alcanza las "ideas y principios implícitos en los elementos del programa"[147], pues se intenta evitar monopolizar tales ideas. Y como reflejo, el artículo 96.4 TRLPI dispone que "no estarán protegidos mediante los derechos de autor con arreglo a la presente Ley las ideas y principios en los que se basan cualquiera de los elementos de un programa de ordenador incluidos los que sirven de fundamento a sus interfaces". En este sentido, y como recuerda Ortega se ha pronunciado el TJUE en el asunto C-406/2010 SAS Institute Inc. vs. World Programming Ltd[148]. Y la cuestión no se modifica por la más reciente Directiva 2019/790, de 17 de abril. Eso sí, es muy posible que la cuestión deba variar en un futuro cercano.

El mejor encaje de protección de los algoritmos hoy por hoy curiosamente lo es como secreto industrial o comercial/Know-How[149]. La protección del Know-How, como secreto

---

Patentes. Respecto al ámbito europeo, también se rechaza su patentabilidad por los mismos motivos en el artículo 52 del Convenio de Múnich. La cámara de recursos de la Oficina Europea de Patentes ha rechazado varías solicitudes de patente de algoritmos.

[147] Considerando 11 de la Directiva 2009/24/CE, sobre la protección jurídica de programas de ordenador, esta norma "sólo protege la expresión del programa de ordenador y que las ideas y principios implícitos en los elementos del programa, incluidas sus interfaces, no pueden acogerse a la protección de los derechos de autor con arreglo a la presente Directiva. De acuerdo con este principio de derechos de autor, en la medida en que la lógica, los algoritmos y los lenguajes de programación abarquen ideas y principios, estos últimos no están protegidos con arreglo a la presente Directiva".

[148] Esta STJUE de 2 de mayo de 2012 (Asunto C-406/2010) expresa que no tienen protección del derecho de autor "ni la funcionalidad de un programa de ordenador ni el lenguaje de programación o el formato de los archivos de datos utilizados en un programa de ordenador para explotar algunas de sus funciones constituyen una forma de expresión de ese programa y, por ello, carecen de la sobre los programas de ordenador en el sentido de esta Directiva" (ap. 46).

[149] Como señala Ortega, definido por el Tribunal Supremo, en su STS de 19-12-2002 como "conjunto no divulgado de informaciones técnicas, patentadas o no, que son necesarias para la

industrial, está recogido en la Ley de Competencia Desleal[150], y en el Código Penal (artículos 278 y ss.). El concepto de secreto comercial o empresarial lo define la Directiva 2016/943/UE[151] (art. 2.1) el "secreto comercial" (o "secreto empresarial" en la ley española) por cuanto (1) no sea conocida ni fácilmente accesible, (2) tener valor por ello mismo y (3) con "medidas razonables" para mantenerla en secreto.[152] Y esta definición es fácilmente proyectable a los algoritmos. Es relevante en esta dirección la Ley 1/2019, de 20 de febrero, de Secretos Empresariales, que transpone la Directiva 2016/943/UE, pues su Capítulo III conecta al "secreto empresarial como objeto del derecho de propiedad". I. El punto de partida, pues, "es el derecho de gozar y disponer de una cosa, sin más limitaciones que las establecidas en las leyes" (artículo 348 Código Civil). Se trata de una visión residual mejorable pues el valor y protección jurídica de los mismos no parece que deba darse por su carácter de secretos.

En razón de esta regulación de secretos, en todo caso, se trata de una propiedad transmisible (art. 4)[153] . De la propiedad del secreto puede haber cotitularidad (art. 5). Dicho condominio se hace depender de lo acordado por las partes en primer lugar. Si no

---

reproducción industrial directamente y en las mismas condiciones, de un producto o un procedimiento".

[150] Ley 3/1991, de 10 de enero, de Competencia Desleal, artículo 13. Violación de secretos. Se considera desleal la violación de secretos empresariales, que se regirá por lo dispuesto en la legislación de secretos empresariales.

[151] Directiva (UE) 2016/943 del Parlamento Europeo y del Consejo, de 8 de junio de 2016, relativa a la protección de los conocimientos técnicos y la información empresarial no divulgados (secretos comerciales) contra su obtención, utilización y revelación ilícitas. Artículo 1. 1º "secreto comercial" (o "secreto empresarial", toda información que: sea secreta "no ser, en su conjunto o en la configuración y reunión precisas de sus componentes, generalmente conocida por las personas pertenecientes a los círculos en que normalmente se utilice el tipo de información en cuestión, ni fácilmente accesible para éstas". Asimismo, que tenga valor comercial precisamente por su secreto y que haya esfuerzos razonables para mantenerla en secreto.

[152] "!a) ser secreta en el sentido de no ser, en su conjunto o en la configuración y reunión precisas de sus componentes, generalmente conocida por las personas pertenecientes a los círculos en que normalmente se utilice el tipo de información en cuestión, ni fácilmente accesible para estas;

b) tener un valor comercial por su carácter secreto;

c) haber sido objeto de medidas razonables, en las circunstancias del caso, para mantenerla secreta, tomadas por la persona que legítimamente ejerza su control".

[153] Artículo 4. Transmisibilidad del secreto empresarial. El secreto empresarial es transmisible. En la transmisión habrán de observarse, cuando resulten aplicables por la naturaleza del secreto empresarial, los reglamentos de la Unión Europea relativos a la aplicación del apartado 3 del artículo 101 del Tratado de Funcionamiento de la Unión Europea a determinadas categorías de acuerdos de transferencia de tecnología.

se acuerda nada hay un régimen por defecto sobre la explotación, conservación, ejercicio de acciones [154]. Para la cesión o concesión de licencia se tiene que otorgar conjuntamente, a salvo de resolución judicial[155]. Respecto de las licencias de los secretos rige lo pactado, y a partir de ahí la regulación del artículo 6. En principio la licencia implica todo acto, la licencia se presume que no es exclusiva. Si es exclusiva no se puede otorgar otras licencias y quien otorga la licencia tampoco podrá utilizar el secreto. El secreto habrá de mantenerse por quien logra la licencia[156]. Finalmente, el artículo 7 salvo pacto se impone responsabilidad por daños al transmitente de licencia.[157] Amén de estas

---

[154] 1. El secreto empresarial podrá pertenecer pro indiviso a varias personas. La comunidad resultante se regirá por lo acordado entre las partes, en su defecto por lo dispuesto en los apartados siguientes y, en último término, por las normas de derecho común sobre la comunidad de bienes.

2. Cada uno de los partícipes por sí solo podrá:

a) Explotar el secreto empresarial previa notificación a los demás cotitulares.

b) Realizar los actos necesarios para la conservación del secreto empresarial como tal.

c) Ejercitar las acciones civiles y criminales en defensa del secreto empresarial, pero deberá notificarlo a los demás comuneros, a fin de que éstos puedan sumarse a las mismas, contribuyendo en tal supuesto al pago de los gastos habidos. En todo caso, si la acción resultase útil a la comunidad, todos los partícipes deberán contribuir al pago de dichos gastos.

[155] 3. La cesión del secreto empresarial o la concesión de licencia a un tercero para explotarlo deberá ser otorgada conjuntamente por todos los partícipes, a no ser que el órgano jurisdiccional por razones de equidad, dadas las circunstancias del caso, faculte a alguno de ellos para realizar la cesión o concesión mencionadas.

[156] Artículo 6. Licencias de secretos empresariales.

1. El secreto empresarial puede ser objeto de licencia con el alcance objetivo, material, territorial y temporal que en cada caso se pacte. Salvo pacto en contrario, el titular de una licencia contractual tendrá derecho a realizar todos los actos que integran la utilización del secreto empresarial.

2. La licencia puede ser exclusiva o no exclusiva. Se presumirá que la licencia es no exclusiva y que el licenciante puede otorgar otras licencias o utilizar por sí mismo el secreto empresarial. La licencia exclusiva impide el otorgamiento de otras licencias y el licenciante sólo podrá utilizar el secreto empresarial si en el contrato se hubiera reservado expresamente ese derecho.

3. El titular de una licencia contractual no podrá cederla a terceros, ni conceder sublicencias, a no ser que se hubiere convenido lo contrario.

4. El licenciatario o sublicenciatario estará obligado a adoptar las medidas necesarias para evitar la violación del secreto empresarial.

[157] Artículo 7. Transmisión o licencia sin titularidad o facultades.

cuestiones, en la ley se regulan expresamente las acciones de defensa de los secretos empresariales, así como cuestiones de la jurisdicción y procedimiento aplicables.

Respecto de las bases de datos resulta muy difícil ubicarlas como base de datos protegidas por propiedad intelectual (art. 12 LPI), pues se requiere que sea original en cuanto a la estructura y la disposición de sus contenidos (12.1 LPI). Sin embargo, los datos son recopilados y procesados de manera automática. No existe una intervención humana que pueda ser considerada una creación intelectual. Tampoco es sencillo atribuir la protección especial de base de datos por el derecho sui generis artículos 133-136 LPI, puesto que lo que se protege es la inversión en la obtención de los datos, pero no en su producción.

Se concluye que hoy por hoy algoritmos y bases de datos pueden considerarse como secretos comerciales, y estar protegidos tanto por la Directiva como por la Ley 3/1991, de 10 de enero, de Competencia Desleal.

> "Artículo 13. Violación de secretos. 1. Se considera desleal la divulgación o explotación, sin autorización de su titular, de secretos industriales o de cualquier otra especie de secretos empresariales a los que se haya tenido acceso legítimamente, pero con deber de reserva, o ilegítimamente, a consecuencia de alguna de las conductas previstas en el apartado siguiente o en el artículo 14. 2. Tendrán asimismo la consideración de desleal la adquisición de secretos por medio de espionaje o procedimiento análogo. 3. La persecución de las violaciones de secretos contempladas en los apartados anteriores no precisa de la concurrencia de los requisitos establecidos en el artículo 2. No obstante, será preciso que la violación haya sido efectuada con ánimo de obtener provecho, propio o de un tercero, o de perjudicar al titular del secreto".

Ello, no obstante, genera algunas cuestiones, especialmente por cuanto a la protección del big data, precisamente para no ser un obstáculo al desarrollo y a la competencia[158].

Quien transmita a título oneroso un secreto empresarial u otorgue una licencia sobre el mismo responderá, salvo pacto en contrario, frente al adquirente de los daños que le cause, si posteriormente se declarara que carecía de la titularidad o de las facultades necesarias para la realización del negocio de que se trate. Responderá siempre cuando hubiera actuado de mala fe.

[158] Miralles Miravet Sergio, Big Data, un nou bé jurídic? En *Món jurídic* … p. 19

Y deben reunirse unos requisitos en razón de la Directiva 2016/943 relativa a la protección de los conocimientos técnicos y la información empresarial no divulgados (secretos comerciales) contra su obtención, utilización y revelación ilícitas:

- Ser secreta.
- Tener un valor comercial ya sea real o potencial.
- Haber sido objeto de medidas razonables, en las circunstancias del caso, para mantenerla secreta[159].

Ante la incertidumbre jurídica **es de interés establecer un marco contractual en las relaciones de los institutos y organizaciones**. En estos marcos es posible dejar más claras las facultades y poder de disposición que tienen las partes respecto de los datos y los algoritmos a los que se acceda o se pongan a disposición de otras partes y terceros.

En 2019 se aprobó la Directiva (UE) 2019/790 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, sobre los derechos de autor y derechos afines en el mercado único digital y por la que se modifican las Directivas 96/9/CE y 2001/29/CE. En sus considerandos 8 y 9 se mencionan las dificultades para señalar la necesidad de autorización por el titular de derechos para la realización de la minería de datos[160] y las flexibilizaciones y excepciones que deben darse para los usos con fines de investigación científica. En particular hay que seguir los mandatos de regulación de los artículos 4 y 5.

Considerando 8 "…No obstante, esos organismos e instituciones se enfrentan en la Unión a cierta inseguridad jurídica a la hora de determinar hasta qué punto pueden llevar a cabo actividades de minería de textos y datos de contenidos. En determinados casos, la minería de textos y datos puede comportar actos protegidos por derechos de autor, por el derecho sui generis sobre las bases de datos, o por ambos, en particular, la reproducción de obras u otras prestaciones, la extracción de contenidos de una base de datos, o ambos, lo que sucede, por ejemplo, cuando se normalizan los datos en el proceso de minería de textos y datos. Cuando no se aplica ninguna excepción o limitación, se requiere una autorización de los titulares de derechos para llevar a cabo tales actos."

[159] Ortega, *ibídem*.

[160] La misma se define como "«minería de textos y datos»: toda técnica analítica automatizada destinada a analizar textos y datos en formato digital a fin de generar información que incluye, sin carácter exhaustivo, pautas, tendencias o correlaciones". (art. 2.2 Directiva (UE) 2019/790).

> Considerando 9. "La minería de textos y datos también puede tener por objeto meros hechos o datos que no están protegidos por derechos de autor y, en tales casos, no se necesita una autorización con arreglo al Derecho en materia de derechos de autor. También puede haber casos de minería de textos y datos que no conlleven actos de reproducción o en los que las reproducciones estén contempladas en la excepción obligatoria aplicable a los actos de reproducción provisional, establecida en el artículo 5, apartado 1, de la Directiva 2001/29/CE, que debe seguir aplicándose a las técnicas de minería de textos y datos que no requieran la realización de copias más allá del alcance de dicha excepción."

A falta de una regulación más concreta sobre el tema, es de interés tener en cuenta la clara voluntad de la UE de facilitar el uso para la investigación de grandes datos, también en el marco de la colaboración público-privada:

> Considerando 11. "La inseguridad jurídica en materia de minería de textos y datos debe subsanarse estableciendo una *excepción obligatoria para las universidades y otros organismos de investigación*, al igual que las instituciones responsables del patrimonio cultural, *respecto del derecho exclusivo de reproducción y del derecho de prohibir la extracción de una base de datos*. En consonancia con la actual política de investigación de la Unión, que anima a las *universidades y los institutos de investigación a colaborar con el sector privado, los organismos de investigación también han de poder acogerse a la excepción cuando sus actividades de investigación se lleven a cabo en el marco de asociaciones público-privadas.* Si bien los organismos de investigación y las instituciones responsables del patrimonio cultural han de seguir siendo los beneficiarios de dicha excepción, deben también poder recurrir a sus socios privados para realizar la minería de textos y datos, también mediante la utilización de sus medios tecnológicos."

En cualquier caso, se trata de una cuestión jurídica que requiere un análisis particularizado en cada caso y dependiente de la transposición de la Directiva en el ordenamiento jurídico español de los mencionados artículos 3 y 4.

XVI. ÉTICA Y CUMPLIMIENTO NORMATIVO ESPECÍFICO EN INTELIGENCIA ARTIFICIAL

1. Ética de la IA en la UE y la Lista de evaluación para una IA fiable

Son ya diversos los hitos y documentos de la llamada Ética de la IA[161] en el mundo[162]. En el ámbito de la UE son múltiples y muy activos los diversos focos de actuación. Ya el 16 de

[161] Sobre el tema, puede seguirse Cotino Hueso, Lorenzo, "Ética en el diseño para el desarrollo de una inteligencia artificial, robótica y big data confiables y su utilidad desde el derecho" en *Revista Catalana de Derecho Público* nº 58 (junio 2019). http://revistes.eapc.gencat.cat/index.php/rcdp/issue/view/n58

[162] El IEEE (Instituto de Ingenieros Eléctricos y Electrónicos), la organización técnica profesional más grande del mundo, En diciembre de 2016 (IEEE, 2016-2017) lanzó la primera versión del documento de políticas del IEEE sobre el "diseño éticamente alineado", actualizados en diciembre de 2017. Más de 250 líderes de opinión mundiales fueron consultados en las primeras ediciones. Desde la International Telecommunication Union (ITU) desde 2017 se lideran las cumbres anuales AI for Good que culminan con documentos y declaraciones relevantes (ITU, 2017). Asimismo, la ACM's (Association for Computing Machinery) también desde 2017 realiza conferencias sobre IA, ética y sociedad (www.aies-conference.com). De particular relevancia, la Alianza sobre la IA ("Partnership on AI, 2018") reúne a más de 80 entidades públicas y privadas entre las que se encuentran las grandes compañías tecnológicas, proclamando 7 principios en septiembre de 2018. También, especialmente dedicada a la investigación de la IA para el bien común, destaca Open AI (https://openai.com) con empresas e investigadores muy destacados. Una actividad significativa desde 2015 la ha realizado el Future of Life Institute (https://futureoflife.org/team), destacando la movilización para evitar una escalada de la IA en el armamento. La Conferencia de enero de 2017 (Asilomar, 2017) concluyó afirmando 23 principios sobre cuestiones de investigación (5), ética y valores (6-18) y problemas a largo plazo. La Universidad de Montreal lideró también un proceso participativo que llevó a un primer borrador de "Declaración para un Desarrollo Responsable de la Inteligencia Artificial" (Montreal Declaration 2017) proclamando 10 principios. Desde Naciones Unidas cabe destacar el centro UNICRI de Inteligencia Artificial y Robótica en La Haya del que han surgido diversos estudios y la Unesco ha adoptado un papel activo , al tiempo de cerrar estas páginas aboga por un "enfoque humanístico" y una gobernanza de la IA que respete los derechos .

En el ámbito internacional de la protección de datos destaca inicialmente International Working Group on Data Protection in Telecommunications (2014). En este foro se adoptó en 2014 el Documento de trabajo sobre "Big Data y privacidad, principios de privacidad bajo presión en la era del análisis de Big Data" (Skopje, 5-6 Mayo de 2014). Destaca en cualquier caso la actividad de la Conferencia Internacional de Autoridades de Protección de Datos (ICDPPC). Las amenazas del big data fuero objeto de una breve resolución de dos páginas en la 36 Conferencia, celebrada en 2014 en Isla Mauricio (ICDPPC, 2014). Y de modo concreto, para la 38 Conferencia Internacional de Marrakech se elaboró un documento de trabajo "Room Document" sobre el tema (ICDPPC, 2016). Sobre esta base, destaca finalmente la Declaración

septiembre de 2014, las autoridades de protección de datos de los Estados de la UE en el antiguo Grupo del Artículo 29 (2014) adoptaron la "Declaración sobre el impacto del desarrollo de big data en la protección de las personas con respecto al procesamiento de sus datos personales en la UE".

El Parlamento Europeo destaca por su importante Resolución, de 16 de febrero de 2017[163], sobre normas de Derecho civil sobre robótica y un importante anexo de principios y códigos de conducta. Y al mes siguiente se adoptó la no menos importante Resolución del Parlamento Europeo, de 14 de marzo de 2017, sobre las implicaciones de los macrodatos en los derechos fundamentales.[164]

La Comisión Europea (2018 a) en abril de 2018 publicó su Comunicación "Inteligencia artificial para Europa". También de la Comisión Europea (2018 b) destaca el "Plan coordinado sobre la Inteligencia artificial" de 7 de diciembre de 2018 así como su importante Anexo (Comisión Europea, 2018 c) con el especial énfasis puesto en una IA "Made in Europe" y "confiable". El mayor distintivo de esta marca Europa es el "*Ethics & Rule of law by design* X-by design" (AI-HLEG, 2018: 19).

En abril de 2018, la Comisión nombró 52 miembros del Grupo de expertos de alto nivel en IA (en adelante AI HLEG, 2018-2019)[165]. Además de afirmar los principios éticos resulta especialmente destacable la visión más práctica que afirma los "requisitos de la IA de confianza" y los "Métodos técnicos y no técnicos para lograr una IA confiable" (AI HLEG, 2018: 14-24).

Precisamente en la versión definitiva el *check list* para comprobar una IA confiable (pp. 33 y ss.). Se trata de un documento que se incluye en el Anexo de esta Guía pues implica a modo de un Estudio de impacto con 150 cuestiones a analizar previamente en todo proyecto de inteligencia artificial para cumplir con los estándares que se están afianzando en la UE.

---

sobre Ética y Protección de Datos en el Sector de la Inteligencia Artificial en el marco de la 40 Conferencia Internacional de Bruselas, de octubre de 2018.

[163] Parlamento Europeo *Normas de Derecho civil sobre robótica. Resolución del Parlamento Europeo*, de 16 de febrero de 2017, con recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica (2015/2103(INL)). Acceso en http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2017-0051+0+DOC+XML+V0//ES

[164] Parlamento Europeo, Resolución de 14 de marzo de 2017, sobre las implicaciones de los macrodatos en los derechos fundamentales: privacidad, protección de datos, no discriminación, seguridad y aplicación de la ley (2016/2225(INI)). Acceso en http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2017-0076+0+DOC+XML+V0//ES

[165] https://ec.europa.eu/digital-single-market/en/high-level-expert-group-artificial-intelligence

La "Lista de evaluación para una IA fiable (AI HLEG UE 2019, versión piloto) (ver ANEXO) agrupa las cuestiones a analizar es siete grupos.

1. Acción y supervisión humanas
2. Solidez técnica y seguridad
3. Gestión de la privacidad y de los datos
4. Transparencia
5. Diversidad, no discriminación y equidad
6. Bienestar social y ambiental
7. Rendición de cuentas

Por su parte, la Agencia de Derechos Fundamentales[166] ya lanzó un estudio específico sobre sesgos y discriminación algorítmica y en diciembre 2020 uno específico de inteligencia artificial y derechos fundamentales.

2. Los principios de la ética de la inteligencia artificial, códigos de conducta profesionales y licencias para diseñadores y usuarios

El punto de partida y premisa ética de la IA en las numerosas declaraciones y documentos los diferentes documentos no es otro que la dignidad y los derechos fundamentales.

Los cinco principios básicos a los que se reconducen los principios éticos reconocidos internacionalmente. La declaración del Parlamento UE (2017 a) sobre robótica es buena expresión de lo que constituyen los principios éticos esenciales.

Así, además del **"principio de transparencia"** (nº 12) y señala que "este marco de orientaciones éticas debe basarse en los principios de **beneficencia, no maleficencia, autonomía y justicia,** así como en los principios consagrados en la Carta de los Derechos Fundamentales de la Unión Europea […] así como en otros principios […] como la no estigmatización, la transparencia, la autonomía, la responsabilidad individual, y la

[166] FRA, Agencia de Derechos Fundamentales UE. (2018). *#BigData: Discrimination in data-supported decision making*, European Union Agency for Fundamental Rights, Viena, Acceso en https://fra.europa.eu/en/publication/2018/big-data-discrimination

FRA, Agencia de Derechos Fundamentales UE. (2020). *Getting the future right artificial intelligence and fundamental rights*, https://fra.europa.eu/en/publication/2020/artificial-intelligence-and-fundamental-rights resultan de interés sus anexos: Acertando el futuro: inteligencia artificial y derechos fundamentales - Anexo I: Metodología de investigación y Ejemplos de evaluación teórica del daño y el impacto significativo de la IA o las decisiones automatizadas.

responsabilidad social" (nº 13). Esto es, ya condensó en buena medida todos los principios en estos cinco.

> En 2018, el proyecto AI4People ha llegado a contabilizar 47 principios éticos proclamados internacionalmente. Y considera que hay cinco principios que sintetizan o captan el significado de 47 [167]:
>
> - beneficencia ("hacer el bien"), no maleficencia ("no hacer daño"),
> - autonomía o acción humana ("human agency") ("respeto por la autodeterminación y elección de los individuos") y
> - justicia ("Trato justo y equitativo para todos").
> - A éstos cuatro añade el también mencionado por el Parlamento, principio de explicabilidad o transparencia ("operar de modo transparente" o como "inteligibilidad y responsabilidad").

El alto grupo de expertos de la UE los asume directamente por su carácter inclusivo y, sobre todo, porque "estos principios generales proporcionan una guía hacia la operacionalización de los valores fundamentales[168]. Los cinco principios pasan a ser hoy día los pilares de la IA confiable *Made in Europe*.

Los cuatro principios esenciales y el de transparencia van acompañados de **otros principios básicos**.

> El Parlamento UE (2017 a) en su anexo código de conducta para ingenieros de robótica afirma otros principios como los de precaución; participación; rendición de cuentas; seguridad; reversibilidad e inversión de acciones y volver a la fase "buena" de su trabajo; privacidad y maximización de beneficios y reducir al mínimo los daños.
>
> Asimismo, en el código de comités de ética incluye principios como evitar conflictos de intereses; acreditada competencia y experiencia de sus miembros, independencia, transparencia y obligación de rendir cuentas, carácter multidisciplinar y como mínimo un miembro con formación filosófica, ética o jurídica.
>
> En el Reino Unido la Cámara de los Lores [169]) parte de "cinco principios generales para un código de IA". Además de beneficencia (1), transparencia o inteligibilidad (2) y no maleficencia-no disminuir derechos (3); incluye la limitación del poder autónomo de los

[167] Floridi, Luciano. *et al.* (2018). "*AI4People* —An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations", *Minds and Machines* 28(4): 689-707. : 696. Acceso en https://doi.org/10.1007/s11023-018-9482-5 y https://link.springer.com/article/10.1007/s11023-018-9482-5

[168] "AI-HLEG, 2018: 8

[169] Cámara de los Lores (2018). AI in the UK: ready, willing and able?, ("AIUK"), nº 417 abril 2018 acceso en https://publications.parliament.uk/pa/ld201719/ldselect/ldai/100/10002.htm

sistemas para herir, destruir o engañar a los seres humanos (5) y el "derecho a ser educados para permitirles prosperar mental, emocional y económicamente junto con la inteligencia artificial" (4).

El **grupo de altos expertos de la UE**[170] afirma diez requisitos y principios de la IA, de entre los subrayar el de responsabilidad (1º), como posible compensación monetaria, en la detección de fallos e incluso simple reconciliación sin compensaciones. El de gobernanza de los datos (2º) pone el énfasis en asegurar la calidad de los datos, la prevención de sesgos y que la anonimización permita la división de los datos en conjuntos. Se insiste en la evitación de datos maliciosos especialmente para que sistemas de autoaprendizaje no entrenen con ellos. Asimismo, la garantía de que los datos recopilados no se utilizarán contra las personas que los proporcionaron. Se afirma también (3º) el principio de diseño para todos, pero no con un enfoque único, sino centrado en el usuario y tener en cuenta toda gama de particularidades.

Resulta de interés el principio de "robustez" ("Robustness", 8º). Con él se reclaman sistemas seguros, confiables y suficientemente sólidos frente errores o inconsistencias durante la fase de diseño, desarrollo, ejecución, implementación y uso del sistema IA, y para enfrentar adecuadamente los resultados erróneos. Se incluyen las exigencias de fiabilidad ("reliability") por cuanto los resultados deben poder ser avalados por evaluación independiente y de reproducibilidad ("reproducibility"): que los resultados sean consistentes en diferentes situaciones, marcos computacionales y datos de entrada. Este principio incluye también la exactitud ("accuracy") para clasificar correctamente la información en las categorías correctas, o su capacidad para hacer predicciones, recomendaciones o decisiones correctas basadas en datos o modelos. Igualmente, la resiliencia frente a las vulnerabilidades y ataques que pueden afectar al funcionamiento mismo del sistema, a las decisiones, su sesgo o generar daños. Asimismo, se exige un "Plan de retroceso" ("Fall back plan") en caso de problemas con el sistema de IA, esto es, que el sistema de IA cambie del procedimiento o directamente que actúe un operador humano.

En el anexo a esta guía se incluye un Código de conducta del Parlamento europeo y licencias para desarrolladores y usuarios. Los mismos pueden servir de pautas de actuación para entidades o estructuras de investigación y experimentación como el Data Space o hubs como el DCH.

3. Regulación jurídica. El régimen de protección de datos se proyecta en muchos casos para la inteligencia artificial

En general no existe una normativa específica para el ámbito más concreto de la inteligencia artificial.

[170] AI-HLEG, 2018: 14-18

Sobre el particular es esencialmente recomendable del Grupo del Artículo 29-UE *Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679*, 3 de octubre de 2017, versión final 6 de febrero de 2018, Doc WP251rev.01. (G29-UE, 2018)

La IA atrae casi por defecto la aplicación del régimen de la protección de datos. Y en ocasiones, es casi el único régimen jurídico hoy día claramente aplicable. En muchos casos la IA implica la elaboración de perfiles, esto es, evaluación automatizada de personas por cuanto su rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física, etc. (art. 4. 4º RGPD). Asimismo, la IA supone también en muchos casos decisiones automatizadas basadas en datos directos, observados o inferidos de las personas[171]. Para que sea aplicable el régimen de protección de datos debe darse la premisa de que los variados macrodatos que *alimentan* la IA sean datos de personas identificadas o identificables, o reidentificables. No se aplicará la normativa si se da una anonimización que garantice que los datos no vuelvan a ser personales[172].

> Si se aplica la normativa de protección de datos a la IA hay que partir del cumplimiento de los principios, la legitimación del tratamiento, los derechos, la responsabilidad proactiva y privacidad en el diseño o el régimen de las transferencias internacionales de datos. Asimismo, y por defecto se exigirá el estudio de impacto.

4. Las garantías más intensas por el nuevo "derecho" a no ser sometido a decisiones automatizadas

El uso de la IA respecto de los humanos es el ámbito potencial de proyección del "derecho" a no ser sometido a decisiones automatizadas. Se trata de un derecho reconocido en el artículo 22 RGPD) de la UE[173] o el artículo 11 de la Directiva (UE) 2016/680 para el ámbito judicial, policial y de seguridad.

La clara intención de este "derecho" es que las decisiones automatizadas relevantes, por su sensibilidad o particularidad, tienen ser compensadas con garantías especiales. Debe señalarse que este "derecho" también supone una prohibición más intensa de tratamientos automatizados si se basan en datos especialmente protegidos.

---

[171] G29-UE, 2018: 7-8

[172] Guía Big Data AEPD-ISMS, 2017, pp. 40 y ss.; Stalla-Bourdillon y Knight, 2017

[173] De especial referencia al respecto son las "Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679" del ya extinto Grupo del Artículo 29, de 3 de octubre de 2017, revisadas el 6 de febrero de 2018.

5. Garantías específicas a adoptar

Pues bien, cabe recordar que el G29-UE[174] detalla diversas de estas garantías. Se trata de una serie de medidas esencialmente "para garantizar que las personas reciben un trato justo y no discriminatorio", sin "resultados discriminatorios, erróneos o injustificados".

Para ello, se señalan como "buenas prácticas" garantías como:

-controles periódicos de calidad de sus sistemas.

-Auditorías algorítmicas: comprobación del funcionamiento y resultados de los algoritmos utilizados y desarrollados por los sistemas de aprendizaje automático.

-Si hay elevado impacto sobre las personas, auditorías independientes de terceros, quienes deben acceder a toda la información necesaria del sistema IA.

- Garantías contractuales respecto de los algoritmos de terceros que garanticen comprobaciones y cumplimiento normativo.

- Medidas específicas para la minimización de datos, claros periodos de conservación.

- Técnicas de anonimización y seudoanonimización respecto de la elaboración de perfiles;

- Formas de permitir al interesado expresar su punto de vista e impugnar la decisión

-mecanismo para la intervención humana en determinados casos, como enlaces a recurso o impugnaciones, plazos determinados, contacto para cualquier consulta.

Asimismo, se apuntan otras opciones como mecanismos de certificación para operaciones de tratamiento; códigos de conducta para procesos de auditoría; comités de ética para evaluar los daños y beneficios.

Resulta de interés tener en cuenta estas garantías enunciadas por el G29-UE y en paralelo el listado de estudio de impacto ético con 150 preguntas que ha incluido la UE en abril de 2019[175] (AI-HLEG (2019).

Este derecho respecto de las decisiones sólo automatizadas relevantes implica también particulares deberes de transparencia. Así, se da la concreta obligación de facilitar "información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado" (art. 13. 2º f y 14. 2º g) RGPD-UE). De igual modo, el derecho de acceso permite solicitar dicha información (artículo 15. 1º. h).

[174] G29-UE (2018): 37-38.

[175] AI-HLEG (2018 y 2019). Draft Ethics Guidelines for Trustworthy AI. Working Document for stakeholders' consultation, Bruselas, 18 de diciembre 2018 y Ethics Guidelines for Trustworthy AI. Working Document for stakeholders' consultation, Bruselas, 8 de abril de 2019. Ahora también en español.

El G29-UE (2018: 35) detalla que la información que debe facilitarse es sobre:

-las categorías de datos que se han utilizado o se utilizarán en la elaboración de perfiles o el proceso de toma de decisiones;

-por qué estas categorías se consideran pertinentes;

-cómo se elaboran los perfiles utilizados en el proceso de decisiones automatizadas, incluidas las estadísticas utilizadas en el análisis;

-por qué este perfil es pertinente para el proceso de decisiones automatizadas; y cómo se utiliza para una decisión relativa al interesado.

También se recomienda informar en general respecto de toda decisión automatizada, aunque no sean las protegidas por el artículo 22 y este derecho G29-UE (2018: 27).

Ahora bien, cabe reiterar que estas garantías en todo caso se añaden o superponen a las que ya confiere el régimen general de protección de datos. Así, respecto de decisiones que no sean sólo automatizadas o no sean relevantes para el afectado, *siempre quedará el París* del régimen general de protección de datos aplicable.

6. Medidas especialmente destinadas a evitar el sesgo o discriminación de la inteligencia artificial

La resolución del Parlamento UE sobre macrodatos "insta" a "minimizar la discriminación y el sesgo algorítmicos" (nº 20) y afirma también la necesaria "mitigación algorítmica" (nº 21, ver también 32). Subraya especialmente que se incluyan mecanismos de transparencia y rendición de cuentas y la posibilidad de corrección de datos y de recurrir decisiones algorítmicas. Y también los propios algoritmos pueden ser el antídoto contra el sesgo algorítmico y se pueden programar para ignorar o minimizar la importancia que los factores prohibidos en sus decisiones.

La minimización, no obstante, debe garantizar que el sistema inteligente no pierda su eficacia, su propia naturaleza o lleve a generar resultados absurdos. Y es que la eliminación o minimización de algunos datos o factores pueden hacer disfuncionales o incluso inservibles los perfilados, clasificaciones, correlaciones o predicciones.

Frente a la discriminación algorítmica hay que extender el modelo de la responsabilidad proactiva en protección de datos, la no discriminación en el diseño y por defecto, así como medidas concretas en los estudios de impacto. Precisamente, varias de las "buenas prácticas" arriba enunciadas que el G29-UE (2018: 36) incluye como garantías respecto de las decisiones automatizadas son frente a la discriminación. Igualmente, no pocas de las 150 **cuestiones del *checklist* en las Directrices** (**ANEXO**) para la ética en el diseño en la UE lo son para lograr la exactitud y fiabilidad, integridad, calidad de los datos y para evitar el sesgo y la discriminación (AI-HLEG 2019: 26-31).

Cabe asimismo remitir a excelentes estudios en la materia.[176]

Así, en el **bloque sobre robustez técnica y seguridad** (2) se incluyen cuestiones para asegurar la exactitud y fiabilidad (¿Ha implementado medidas para garantizar que los datos utilizados sean completos y estén actualizados ?; ¿Se implementaron medidas para evaluar si se necesitan datos adicionales, por ejemplo, para mejorar la precisión o para eliminar el sesgo ?; ¿Se verificó qué daño se causaría si el sistema de AI hace predicciones inexactas? ¿Se dispusieron formas de medir si el sistema está haciendo una cantidad inaceptable de predicciones inexactas? ¿pasos para aumentar la precisión del sistema?

En el **bloque 3 sobre privacidad** hay cuestiones sobre la calidad e integridad de los datos (¿Estableció mecanismos de supervisión para la recolección, el almacenamiento, el procesamiento y el uso de los datos ?, ¿Evaluó la medida en que tiene el control de la calidad de las fuentes de datos externas utilizadas? ¿Ha implementado procesos para garantizar la calidad e integridad de sus datos? ¿Consideró otros procesos? ¿Cómo está verificando que sus conjuntos de datos no hayan sido comprometidos o pirateados?).

Y precisamente hay un **bloque sobre "Diversidad, no discriminación y equidad"** (5) con 19 cuestiones. Diversas de las cuales giran sobre "Evitación del sesgo injusto" (¿Estableció una estrategia o un conjunto de procedimientos para evitar crear o reforzar un sesgo injusto en el sistema AI, tanto en el uso de los datos de entrada como en el diseño del algoritmo ?, diversidad y representatividad en los datos; inclusión poblaciones específicas, uso de pruebas en las fases de desarrollo, incorporación de mecanismos específicos para que otros puedan identificar problemas de sesgo o discriminación; mecanismos para consultar estos problemas; consideración de afectados indirectos. Evaluación si variación de resultados en mismas condiciones, cómo medirlo. ¿Cómo se ha medido la imparcialidad?

De igual modo se incluyen en este **bloque cuestiones sobre accesibilidad** y diseño universal (si el sistema de AI es utilizable por personas con necesidades especiales; si la información sobre el sistema de AI es accesible; si en la elaboración se involucró o consultó a esta comunidad; si el equipo de desarrolladores es representativo de su público objetivo; si se evaluó si podría haber personas o grupos que pudieran verse afectados de manera desproporcionada por implicaciones negativas, si se recibieron comentarios de otros equipos o grupos).

El **bloque sobre bienestar social y ambiental** (6) cuenta con alguna cuestión sobre si, por ejemplo, se tuvo en cuenta el impacto social general, como pérdidas de empleo.

Finalmente, en el **bloque de responsabilidad** (7, auditabilidad y documentación de las compensaciones) también se incluyen cuestiones sobre auditoría independiente, evaluación de riesgo o impacto, capacitación y educación, introducción de mecanismos de "junta de revisión ética de AI" o similares. Vinculado a la minimización del sesgo se hace referencia a la posibilidad de compensaciones "trade-off": ¿Estableció un mecanismo para identificar los intereses y valores relevantes implicados por el sistema

[176] Decisiones automatizadas y discriminación: aproximación y propuestas generales", en Revista General de Derecho Administrativo, Nº. 56, 2021 y tesis doctoral de esta autora sobre el tema https://roderic.uv.es/handle/10550/77050

de AI y las posibles compensaciones entre ellos?" Asimismo, se señala la necesidad de documentar la decisión de compensación.

GLOSARIO

Se facilita a continuación un glosario que puede ser de utilidad para la mejor comprensión y seguimiento de esta guía, esencialmente a partir de la Guía de la CRUE[177] y la Guía Requisitos para auditorías de tratamientos de datos personales que incluyan Inteligencia Artificial.

El artículo 4 del RGPD incluye las definiciones de los conceptos básicos en protección de datos. Jurídicamente hay que partir de las mismas pues pueden implicar matices importantes. No obstante, una aproximación no centrada en juristas invita a seguir unos conceptos más próximos o comprensibles.

Para ello se siguen los conceptos de la CRUE en la mencionada Guía, en algunos casos, directamente las definiciones del RGPD.

Anonimización

Es la disociación definitiva e irreversible de los datos personales. Proceso encaminado a convertir los datos en anónimos y romper su vínculo con la persona a la que se refieren, de manera que esta no sea identificable a través de ellos.

Aprendizaje supervisado (*supervised Learning*)

Un operador actúa como “instructor” introduciendo datos etiquetados de entrenamiento en el sistema que contienen los datos de entrada y también los datos de salida “correctos” para esos datos de entrada. El sistema en futuras ocasiones debe seguir la misma lógica.

Aprendizaje no supervisado (*unsupervised Learning*)

No existe realimentación por un operador. Los componentes se diseñan para ser capaces de detectar patrones y reglas latentes en los datos y para resumir y agrupar las unidades de información que conforman los datos.

Aprendizaje semi-supervisado (*semi-supervised Learning*)

Estos suponen un compromiso entre los dos anteriores. Contienen algunos datos de entrada etiquetados, aunque la mayoría de ellos no lo están, complementándose con procedimientos automáticos.

[177] Pp. 73 y ss.

Aprendizaje por refuerzo (*reinforcement Learning*)

El sistema analiza y valora diferentes posibles actuaciones, con el objetivo de determinar, de forma automática, la más idónea dentro de un contexto específico. La señal de refuerzo (reinforcement signal) consiste en una retroalimentación simple que el sistema toma como "recompensa" y permite determinar cómo de "adecuado" es un determinado comportamiento.

Auditoría

Proceso sistemático, independiente y documentado para obtener registros, declaraciones de hechos o cualquier otra información y evaluarlas para determinar el grado en que se cumplen los criterios de auditoría.

Bloqueo de datos

El bloqueo de los datos[178] consiste en la identificación y reserva de los mismos, adoptando medidas técnicas y organizativas, para impedir su tratamiento, incluyendo su visualización, excepto para la puesta a disposición de los datos a los jueces y tribunales, el Ministerio Fiscal o las Administraciones Públicas competentes, en particular de las autoridades de protección de datos, para la exigencia de posibles responsabilidades derivadas del tratamiento y solo por el plazo de prescripción de las mismas. Transcurrido ese plazo deberá procederse a la destrucción de los datos.

Ciclo de vida de un componente IA

Conjunto de etapas en el que se estructura la evolución de este desde su concepción hasta su retirada, podrán ser, en el caso de aprendizaje automático:

- preprocesamiento, en la que se trabaja sobre las bases de datos que servirán para el entrenamiento y la prueba del sistema y que pueden tener datos incompletos, desestructurados y en diferentes formatos, por lo que lo primero de todo será prepararlos para su aprovechamiento. Estos datos se separan generalmente en dos conjuntos: los utilizados para generar el modelo de aprendizaje y los utilizados para su validación.

- preparación del código del componente, que posteriormente se entrena, para generar el modelo algorítmico. La técnica de aprendizaje escogida dependerá de la naturaleza del problema.

- validación sobre el conjunto disjunto de los datos de entrenamiento reservados para este fin.

[178] En este caso voz del Código de Conducta UNED.

- etapas sucesivas de implementación en un modelo comercial, inclusión en un tratamiento, paso a producción, actualización o mantenimiento y finalmente una etapa de retirada.

Es habitual que este modelo de desarrollo cuente con un proceso iterativo de comprobación – reaprendizaje del comportamiento del componente utilizando para ello datos reales que permitan su adaptación y mejora continua.

Comunicación o cesión de datos

Es el tratamiento de datos que supone su revelación a una persona distinta del interesado, excepto el acceso por parte de un encargado de tratamiento a los datos personales que resulten necesarios para la prestación de un servicio al responsable siempre que se cumpla lo establecido en el RGPD, la LOPDGDD y sus normas de desarrollo.

Consentimiento

En aquello supuestos en los que la base jurídica del tratamiento sea el consentimiento, la citada manifestación de voluntad ha de prestarse de forma libre, específica, informada e inequívoca por la que se acepte, mediante una declaración o clara acción afirmativa, el tratamiento de datos que le conciernan al que lo presta. Una de las vías de acreditarlo puede ser mediante la marcación registrada de una casilla de verificación. En cualquier caso, el tratamiento estará limitado a la finalidad para la que se solicita el mismo -art. 5.1.b RGPD-.

Datos biométricos

Son los datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos.

Datos de entrada, datos de salida y datos etiquetados

De entrada (input data) son lo que se introducen en el componente IA para ser procesados por el mismo. De salida (output data), resultan del procesamiento algorítmico de los datos de entrada. Datos etiquetados (labelled data) se introducen en un componente IA y están vinculados a una determinada información de salida.

Datos especialmente protegidos o Categorías especiales de datos personales

Se trata de aquellos datos personales que, por su naturaleza, son particularmente sensibles en relación con los derechos y las libertades fundamentales, ya que el contexto de su tratamiento podría entrañar importantes riesgos para los derechos y las libertades fundamentales. En concreto, lo son los que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una

persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientaciones sexuales de una persona física.

Datos genéticos

Son los datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona.

Datos personales

Toda información sobre una persona física identificada o identificable (el interesado); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

Datos personales identificadores, cuasi-identificadores

Identificadores, datos que, por sí solos, están asociados de forma unívoca a un sujeto como, por ejemplo, el DNI, el nombre completo, el pasaporte, el número de la seguridad social o cualquier otro identificador que cumpla el mismo propósito.

Cuasi-identificadores, también llamados identificadores indirectos o seudo-identificadores, son aquellos datos que, sin identificar directamente al individuo, convenientemente agrupados y relacionados con otros conjuntos de datos o fuentes de información, pueden llegar a identificar a una persona y permitir la vinculación o inferencia con datos sensibles. Suelen entrar en la categoría de estos datos la fecha de nacimiento, el municipio de residencia, el código postal o el género por ser datos muy comunes a un amplio espectro de conjuntos de datos, muchos de ellos de carácter público, en las que puede estar incluido un determinado individuo.

Datos relativos a la salud

Son los datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud.

Deber de confidencialidad

Todas las personas que intervengan en cualquier operación de tratamiento están sujetas al principio de integridad y confidencialidad establecido en el art. 5.1.f) RGPD, con independencia del deber de secreto profesional que se le exija de conformidad con la legislación aplicable.

Ambas obligaciones se mantendrán aun cuando hubiese finalizado la relación del obligado con el responsable o encargado del tratamiento.

Destinatario

Es la persona física o jurídica, autoridad pública, servicio u otro organismo al que se comuniquen datos personales, se trate o no de un tercero. No obstante, no se considerarán destinatarios las autoridades públicas que puedan recibir datos personales en el marco de una investigación concreta de conformidad con el Derecho de la Unión o de los Estados miembros.

Discriminación algorítmica, grupal y estadística

Algorítmica, tratamiento desigual que un componente IA da a una persona X con respecto a otra persona y como consecuencia de un atributo particular de X.

Grupal, afecta a una persona a causa de su pertenencia a un grupo socialmente identificable o protegido.

Estadística, discriminación grupal basada en un hecho que es estadísticamente relevante102

Elaboración de perfiles (perfilado)

Toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física. Se caracteriza por tres elementos: forma automatizada, respecto a datos personales para evaluar aspectos personales sobre una persona física.

Encargado del tratamiento o encargado

La persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento.

Fichero

Todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica.

Interesado

Es la persona física titular de los datos personales.

Minimización de datos

La cesión o comunicación de datos personales, cuando exista base jurídica para ello, debe limitarse a aquellos que sean adecuados, pertinentes y estrictamente necesarios para la finalidad pretendida.

Obligaciones del cesionario

Cuando se revelan o comunican datos personales a terceros, estos quedan sujetos a la normativa de protección de datos personales y a los efectos legales que de ella se deriven en el tratamiento de datos que realice, sin que puedan tratar los datos personales para finalidades distintas para las que se le autorizó la comunicación.

Reidentificación (riesgo de)

Análisis de datos para encontrar propiedades que puedan aumentar el riesgo de que los sujetos sean identificados. Se pueden utilizar para ayudar a determinar una estrategia eficaz de desidentificación o después de la desidentificación para vigilar cualquier cambio o valores atípicos.

Responsable del tratamiento o responsable

la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros.

Responsabilidad proactiva

El Responsable del tratamiento es el encargado del cumplimiento de la normativa y debe ser capaz de demostrarlo.

Seudonimización

Es el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable.

Sesgo algorítmico

Un determinado componente IA produce distintos resultados con relación a los sujetos en función de la pertenencia de este a un colectivo concreto (explícito o ad-hoc) evidenciando un prejuicio subyacente a dicho colectivos: sesgo en los datos de entrenamiento, en la metodología de entrenamiento (p.ej. por una supervisión que incluye el sesgo), por un

modelo demasiado simplista (underfitting), por una aplicación del componente IA en un tratamiento o un contexto que no es adecuado, etc.

Tercero

Persona física o jurídica, autoridad pública, servicio u organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable o del encargado.

Tratamiento

Cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.

Tratamientos de datos personales desde el ciclo de vida IA

Cuando se utilizan datos personales en la etapa de desarrollo del componente IA.

Cuando se utilizan datos personales en las etapas de verificación o validación del componente IA.

Cuando se incluye el componente IA en un tratamiento de datos personales (etapa de explotación), como podría ser un tratamiento de control de seguridad (que incluye reconocimiento facial) o de atención al ciudadano (que incluye en chatbot).

En cualquier otra etapa del ciclo de vida que involucre datos personales.

En dichos tratamientos se podrían utilizar conjuntos de datos (datasets) y se podrían inferir nuevos datos personales. Todos ellos, directos o indirectos, originales o derivados, son datos personales en tanto y cuanto hagan referencia a un individuo identificado o identificable

Violación de la seguridad de los datos personales

toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

ANEXOS

Anexo I. Algunas recomendaciones de la CRUE específicas para ámbitos académicos y universitarios

Anexo II. Cuestionario evaluación proyectos investigación y modelo de Hoja de información

Anexo III. Lista de evaluación para una inteligencia artificial fiable (Grupo de expertos UE 2019, versión piloto)

Anexo IV. Parlamento Europeo. Códigos de conducta y licencias de diseñadores y usuarios robótica

ANEXO I. ALGUNAS RECOMENDACIONES DE LA CRUE ESPECÍFICAS PARA ÁMBITOS ACADÉMICOS Y UNIVERSITARIOS

Recomendaciones de la CRUE respecto de tratamiento de datos por uso de medios tecnológicos habituales en los ámbitos académicos y universitarios

La Guía de buenas prácticas de la CRUE[179] hace algunas referencias a supuestos habituales de tratamiento de datos que son habituales en los medios académicos y universitarios. Cabe recordar algunos supuestos.

> Creación de grupos entre profesores y estudiantes con aplicaciones de mensajería instantánea

Se requiere el consentimiento de cada uno de los que vayan a participar en el grupo, al no entrar este supuesto en las restantes bases jurídicas de legitimación del tratamiento.

Buena práctica: resulta recomendable que se empleen los medios técnicos establecidos por la Universidad (por ejemplo, uso de plataformas institucionales de apoyo a la docencia o listas de distribución).

> Acceso de un miembro de la comunidad universitaria a las direcciones IP desde las que se hayan podido conectar a su cuenta profesional, ante la sospecha de que un tercero ha podido efectuar una entrada indebida

Se pretende discriminar los accesos producidos, al detectarse un posible uso indebido de su cuenta.

No procede el citado acceso, puesto que la indagación o investigación del posible acceso indebido corresponde realizarla a los propios servicios informáticos de la Universidad cuando se trata de recursos tecnológicos propiedad de la institución, quienes elevarán sus conclusiones a las autoridades competentes de la Universidad para poner, en su caso, los hechos en conocimiento de las autoridades competentes para la averiguación y persecución de posibles ilícitos. Todo ello, sin perjuicio de las medidas correctoras que la persona interesada pueda adoptar (cambios de contraseña, etc.). Asimismo, el afectado puede también poner los hechos en conocimiento de las autoridades competentes para la averiguación de posibles ilícitos.

[179] Pp. 23 y ss.

> *Solicitud de baja de las listas de distribución de la Universidad*

En las listas de naturaleza institucional (aquellas creadas para divulgación de las noticias de interés general para los miembros de la comunidad universitaria), el ejercicio del derecho de oposición, y el consecuente cese en el tratamiento de los datos personales, haría perder a estas su propia finalidad.

En lo que respecta a las listas específicas creadas para incluir a colectivos singularizados con interés común sobre un tema concreto (integrantes de grupos de investigación, delegaciones de estudiantes, entre otros), debe prevalecer, con carácter general, el derecho de oposición de la persona interesada (art. 21.1 RGPD). Este mismo derecho ha de extenderse a las listas creadas para difusión de información sindical, excepto en los periodos electorales, como ha reiterado la AEPD (por todas, resoluciones TD-0119-2008; TD- 00869-2014; TD-002429-2017).

En cuanto a los servicios de "newsletter" (boletines de noticias), que la universidad pueda ofrecer a cualquier ciudadano, al fundamentarse su base legitimadora en el consentimiento expreso -art. 6.1.a) RGPD y art. 21 de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico-, el interesado tiene el derecho a revocar su consentimiento en cualquier momento, por lo que de ejercerse este derecho tendría que ser dado de baja.

Buena práctica: una vez tramitada la baja, se remitirá automáticamente un mensaje de correo electrónico al solicitante para que la confirme, y evitar así posibles accesos indebidos de terceros que podrían suplantar la identidad del solicitante de la baja.

> *Huella digital y reconocimiento facial en el ámbito laboral*

La jurisprudencia del Tribunal Supremo se ha pronunciado sobre el uso de la biometría en el ámbito laboral, afirmando que "[…] Desde luego, la finalidad perseguida mediante su utilización es plenamente legítima: el control del cumplimiento del horario de trabajo al que vienen obligados los empleados públicos. Y, en tanto esa obligación es inherente a la relación que une a estos con la Administración […], no es necesario obtener previamente su consentimiento ya que el artículo 6.2 de la Ley Orgánica 15/1999 lo excluye en estos casos. Además, no parece que la toma, en las condiciones expuestas, de una imagen de la mano incumpla las exigencias de su artículo 4.1. Por el contrario, puede considerarse adecuada, pertinente y no excesiva" (por todas, STS núm. 5200/2007, de 2 de julio; FJ 7) (RJ 2007/6598).

El Tribunal Europeo de Derechos Humanos (en adelante, TEDH), en su Sentencia de 5 de septiembre de 2017, as. *Barbulescu v. Rumanía*, considera que existe violación del secreto de las comunicaciones en el despido del demandante por la utilización de mensajería instantánea para uso personal en el centro de trabajo al no ser informado sobre la naturaleza y alcance de la vigilancia a la que iba a ser sometido, así como del grado de intrusión en su vida privada y correspondencia.

No obstante, para que la implantación de un sistema de control horario basado en la recogida de este tipo de datos pueda considerarse proporcionada y, por lo tanto, conforme con el principio de minimización, hay que hacer una evaluación del impacto sobre la protección de datos a la vista de las circunstancias concretas en las que se lleve a cabo el

tratamiento para determinar su legitimidad y proporcionalidad, incluido el análisis de la existencia de alternativas menos intrusivas, y establecer las garantías adecuadas. Dándose estas circunstancias, la base legitimadora -si se trata de garantizar el control de cumplimiento del horario- sería el art. 9.2.b) en relación con el art. 6.1.c) RGPD.

Como indica la APDCat, en el caso del control de acceso a dependencias o zonas que requieran unas condiciones de seguridad reforzadas, el uso de este tipo de sistemas puede resultar justificado en determinados casos, si bien también resulta necesario llevar a cabo con carácter previo la evaluación del impacto en la protección de datos (dictamen CNS 63/2018).

En cualquier caso, en lo que respecta a la huella dactilar, se recomienda que superado el juicio de proporcionalidad se instalen preferentemente aquellos sistemas de reconocimiento que permitan que los medios de verificación (algoritmo de la huella dactilar del trabajador), permanezcan en poder de los afectados, sin ser incorporados al sistema, que incluiría los datos identificativos del trabajador al producirse una verificación positiva del mismo, tal y como se recuerda por la Agencia Vasca de Protección de Datos (en adelante, AVPD) (dictamen CN 16-029). En términos análogos se pronuncia la AEPD (informe 0065/2015).

> Sistemas biométricos de identificación de la persona para fines no laborales

El control de acceso de las personas a las instalaciones estaría legitimado en el art. 6.1.e) RGPD (garantía de la seguridad de las personas, bienes e instalaciones). Sin embargo, hay que analizar si el uso de sistemas biométricos de identificación de las personas para estos fines (por ejemplo, para preservar la seguridad de acceso a las bibliotecas universitarias, asistencia a clase, acceso a comedores, entre otros) es adecuado, pertinente y limitado a lo necesario en relación a estos. En otras palabras, habría que determinar si no hay medios menos intrusivos en la intimidad de las personas, como indica la AEPD, a la vista de la evaluación de impacto que se realice (informe 0065/2015).

Por ejemplo, no sería acorde con los principios contemplados en el art. 5 RGPD el tratamiento de los datos de reconocimiento facial de los estudiantes de los centros universitarios para el control de su asistencia a las clases y de su efectiva participación en las pruebas que se desarrollen en el centro, tal y como pone de manifiesto la AEPD (informe 0392/2011).

Recomendaciones de la CRUE respecto del tratamiento de imágenes con fines de investigación, educativos, institucionales o culturales

Sobre el tratamiento de imágenes[180], no es excesiva la atención en la Guía de la CRUE, si bien cabe remitir en general a todo lo afirmado sobre tratamiento de datos para la investigación.

> Captación y grabación de imágenes para fines de investigación científica

Se requerirá el previo consentimiento del afectado, salvo que resulte de aplicación cualquier otra base de legitimación. Hay que recordar que el tratamiento de datos personales como las imágenes con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, estará sujeto a las garantías adecuadas para los derechos y libertades de los interesados, disponiendo de medidas técnicas y organizativas, en particular para garantizar el principio de minimización de los datos personales, pudiendo incluir la "seudonimización", siempre que de esa forma puedan alcanzarse dichos fines (art. 89 RGPD).

Al respecto del tratamiento de imágenes[181], se abordan algunos supuestos:

> Elaboración de videotutoriales por los estudiantes y posterior publicación en el blog de la Universidad

La elaboración y ulterior publicación de los videotutoriales se ha de fundamentar en el previo consentimiento otorgado por los estudiantes o personas que aparezcan en los videos, salvo que se trate de personas que ejerzan un cargo público o una profesión de notoriedad o proyección pública y la imagen se capte durante un acto público o en lugares abiertos al público (art. 8.2.a Ley Orgánica 1/1982, de 5 de mayo, de protección civil de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, en adelante LO 1/1982).

> Exposición o estand con fotos captadas en actos y eventos de la universidad

La divulgación de las fotos (si en ellas aparecen datos personales) es una comunicación de datos, para la que sería necesario el previo consentimiento de las personas fotografiadas, salvo que ejerzan un cargo público o una profesión de notoriedad o proyección pública y la imagen se capte durante un acto público o en lugares abiertos al público (art. 8.2.a LO 1/1982).

Utilización de imágenes de los miembros de la comunidad universitaria o de terceras personas en acciones promocionales de la Universidad, en memorias, guías, revistas,

[180] P. 32 y ss.

[181] P. 27 y ss

proyectos de innovación docente con fines de difusión de la metodología en entornos académicos o científicos externos, entre otros.

Para la divulgación de las imágenes se requiere el previo consentimiento de los afectados, salvo que resulte de aplicación cualquier otra base de legitimación.

> Publicación de fotos de antiguos alumnos de una determinada promoción

Se requiere el previo consentimiento de los afectados, salvo que resulte de aplicación cualquier otra base de legitimación.

> Grabación de la sesión de una clase en video

En el supuesto de que sea el estudiante el que pretende la grabación será necesario el previo consentimiento de los afectados, incluido el profesor.

Si es el profesor el que está interesado en la grabación será posible, sin previo consentimiento de los asistentes a la clase, si se trata de una grabación que efectúe el docente exclusivamente en el ejercicio de la función educativa en cuyo caso sería de aplicación el artículo 6.1.e) RGPD (tendría su legitimidad legal en la actividad y formación docente prevista en la Ley Orgánica de Universidades), y sin ulterior utilización para otros fines (entre ellas, su divulgación). Las imágenes solo deberán estar accesibles para los estudiantes participantes en dicha actividad y el profesor correspondiente. Si la citada grabación pudiera afectar al derecho al honor, a la imagen o a la intimidad personal de cualquiera de los asistentes, se requeriría su previo consentimiento.

Buena práctica: divulgar a través de las listas institucionales los requisitos para poder proceder a la grabación sin consentimiento expreso y de las responsabilidades en materia de protección de datos que pueden asumirse en caso de incumplimiento, o colocar paneles o carteles informativos en la entrada de las aulas explicando dichos requisitos.

> Uso de imágenes realizadas en actividades académicas, culturales, deportivas, entre otras, correspondientes a actos organizados por la Universidad y su posterior difusión en el canal de noticias de la página web de la Universidad o en las redes sociales institucionales

El hecho de que la realización de las fotos o la grabación de los videos se produzcan durante un acto público no legitima para excluir el previo consentimiento inequívoco de las personas grabadas o fotografiadas, salvo que:

1. Se trate exclusivamente de captar la imagen de los asistentes de forma accesoria y sin posterior divulgación, o

2. Se tomen en un acto de interés histórico, científico o cultural relevante (art. 8.1 de la LO 1/1982).

En lo que respecta al carácter accesorio de las imágenes, hay que tener en cuenta que en estos casos, estrechamente vinculado con el derecho de protección de datos, está el derecho a la propia imagen, que ha sido definido por la jurisprudencia como un derecho que tiene *"cada individuo a que los demás no reproduzcan los caracteres esenciales de su*

figura sin el consentimiento del sujeto, de tal manera que todo acto de captación, reproducción o publicación por fotografía, film u otro procedimiento de la imagen de una persona en momentos de su vida privada o fuera de ella supone una vulneración o ataque al derecho fundamental a la imagen, como también lo es la utilización para fines publicitarios, comerciales o de naturaleza análoga" (STS núm. 256/1999, de 27 de marzo; FJ 3) (RJ 1999/2370).

A la vista de esta doctrina, no sería preciso el consentimiento de los afectados en aquellos supuestos en que su imagen sea captada en relación con un suceso o acontecimiento público y aparezca como meramente accesoria. En ese sentido se han pronunciado la AVPD en su dictamen CN 18-005 y la APDCat en su dictamen CNS 64/2015.

Respecto al carácter accesorio de las imágenes, el artículo 8.2 c) de la LO 1/1982 establece que el derecho a la propia imagen no impedirá *"la información gráfica sobre un suceso o acaecimiento público cuando la imagen de una persona determinada aparezca como meramente accesoria"*. Por su parte, el Alto Tribunal en su STS núm. 220/2014, de 7 de mayo, afirma que *"hay abundante doctrina de esta Sala que toma en cuenta el carácter accesorio de la imagen de una persona, respecto del texto escrito o el contexto de la fotografía o fotograma y que declara que existe tal carácter cuando la imagen no es elemento principal, porque no es necesaria la presencia, ni tiene especial relación con el objeto de la captación o proyección, y no hay nada desmerecedor o de desdoro para el afectado, esta doctrina está ligada siempre a un acontecimiento público"* (FJ 10) (RJ 2014/3299).

El Tribunal Supremo vincula pues el carácter accesorio de una imagen cuando no es necesaria su presencia, estando la intromisión justificada en la medida en que la imagen es captada de manera accidental y secundaria en relación con el resto de la información en la que inserta. En su sentencia núm. 196/2007, de 22 de febrero, el Alto Tribunal se refiere al supuesto de una grabación en video (RJ 2007/1518).

Por consiguiente, concurriendo las circunstancias expuestas, la base legitimadora de la captación de las imágenes por parte de la Universidad en eventos públicos que organice sería el artículo 6.1.e) RGPD. En caso de no estar ante una imagen meramente accesoria o accidental sería necesario el previo consentimiento de los afectados.

Por su parte, se podrá difundir las imágenes captadas en actos académicos relevantes (entre otros, concesión de honoris causa, inauguración del curso académico), cuando afecten a personas que ejerzan un cargo público o una profesión de notoriedad o proyección pública, puesto que se estaría ante un interés público -art. 6.1.e) RGPD- con amparo en el art. 8.2.a) de la LO 1/1982.

En los restantes supuestos, se requiere el consentimiento inequívoco de las personas que aparezcan en las imágenes que se van a divulgar para su posterior difusión pública. En el caso de los menores de catorce años, dicho consentimiento deberá ser otorgado por el titular de la patria potestad o tutela, con el alcance que determinen los titulares de la patria potestad o tutela (art. 7.2 LOPDGDD).

Buena práctica:

- Informar a la entrada del evento de la finalidad de la grabación de imágenes de los asistentes (mediante carteles o paneles informativos, folletos, entre otros).
- Si se cursa invitación se debe advertir de que la Universidad tomará fotografías y/o grabará vídeos.
- Los fotógrafos oficiales deberían de llevar una acreditación que los distinga como tales. Si la captación y uso de imágenes va a ser particularmente intensiva se recomienda repartir algún tipo de distintivo (chapa, pegatina, entre otros) de color entre los asistentes que permita a los fotógrafos evitar a aquellos que no desean ser retratados.
- Los fotógrafos oficiales centrarían la captura de imágenes y vídeos del evento en tomas generales de los asistentes, de forma que ninguno adquiera un papel exclusivo o predominante y la presencia de cualquiera de ellos pueda entenderse como accesoria.

ANEXO II. CUESTIONARIO EVALUACIÓN PROYECTOS INVESTIGACIÓN Y MODELO DE HOJA DE INFORMACIÓN

"Cuestionario/guía para la evaluación de proyectos de investigación con datos por un Comité Ético de investigación

"Cuestionario/guía para la evaluación de proyectos de investigación con datos por un CEI (En cumplimiento del Reglamento Europeo 2016/679 de protección de datos y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales)[182].

1. Aspectos generales a revisar en cada centro

- Que se ha analizado si es necesario realizar una evaluación de impacto en la Protección de Datos Personales (EIPD).
- Que el responsable del tratamiento esté adherido a algún código de conducta o mecanismo de certificación que garantice un nivel de seguridad adecuado al riesgo.
- Que cuente, si es preciso, con el asesoramiento de un delegado de protección de datos.

[182] Alfonso Farnós, Iciar Alcalde Bezhold, Guillermo y Méndez García Miriam, en *Revista de derecho y genoma humano* Nº Extra 1, 2019 (Ejemplar dedicado a: Uso de datos clínicos ante nuevos escenarios tecnológicos y científicos. Oportunidades e implicaciones jurídicas), págs. 25-33.

2. Aspectos que debe revisar un CEI en cada proyecto

		Si No No procede
Protocolo/ memoria científica	• Descripción de la justificación científica y objetivos del estudio; definición de las variables de resultado y del análisis estadístico previsto. • Descripción del tratamiento que va a aplicarse a los datos obtenidos, valoración de los riesgos potencia- les para la privacidad y qué medidas van a adoptarse para reducirlos, aplicando el principio de minimiza- ción de datos (adecuados, pertinentes y limitados a lo necesario en relación a los fines de la investigación).	° ° ° ° ° °

Idoneidad del Investigador/ Responsible del tratamiento	• Se han aportado los documentos que acreditan su formación y experiencia en investigación.
	• Se ha aportado el compromiso escrito referente a:
	  • Utilizar los datos sólo para los fines previs- tos;
	  • Garantizar la confidencialidad de la in- formación y no realizar ninguna actividad de reidentificación de los participantes, ni ceder los datos a terceros no autorizados;
	  • Cumplir las exigencias legales y del comité respecto al seguimiento, informando pe- riódicamente sobre la marcha del estudio.
	• Si se van a tratar los datos seudonimizados se ha aportado un compromiso expreso de confidencialidad y de no realizar ninguna actividad de reidentificación.
	• Se ha aportado la información sobre el encargado del tratamiento de los datos, cuando no coincida con el responsable del tratamiento, en relación a conoci- mientos especializados, fiabilidad y recursos.
	• Se ha firmado un contrato con el encargado del trata- miento.
		° ° °
		° ° °
		° ° °
		° ° °
		° ° °
		Si No No procede

Idoneidad de los medios previstos para el tratamiento de los datos	• Se ha informado sobre las medidas de seguridad para garantizar la privacidad. • Se aporta la información sobre el servidor en el que se van a alojar los datos y las medidas de seguridad que van a adoptarse: a) Se utilizan servidores que cumplen con un plan de gestión de protección de datos, como por ejemplo las bases de datos alojadas en el ser- vidor del centro sanitario/institución/servicio de salud cuando se ha realizado una EIPD. b) Si no se dispone de un plan de gestión de protección de datos se describen las medidas de seguridad adicionales, tanto en el protoco- lo, como en el contrato con el encargado del tratamiento: • Cuadernos de recogida de datos electrónicos (CRFe) ubicados en la web del promotor. • Datos seudonimizados alojados en nubes (Google drive, dropbox, etc.): las plataformas estarán ubicadas en Europa o adscritas al Privacy Shield: https://www.privacyshield.gov/ list. • Se describen las medidas de seguridad de otros medios: software, …	° ° ° ° ° ° ° ° ° ° ° °

3. Aspectos que debe revisar un CEI en cada proyecto

		SI No No procede
Evaluación de las medidas de seguridad previstas en el tratamiento de los datos	• Se informa sobre cómo se accede a los datos. • Se aporta el formulario de recogida de datos/base de datos, en los que se comprueba que no se plan- tea recoger datos identificativos. • Si los datos se recogen codificados se informa sobre quién custodia el código que permitiría la identifi- cación del titular de los datos. • Se aplican los procesos de anonimización y/o seudo- nimización. • Si se tratan los datos seudonimizados se informa so- bre quién y cómo se va a realizar la seudonimización y de las medidas de seguridad específicas que van a adoptarse para evitar la reidentificación y el acceso de terceros no autorizados.	° ° ° ° ° ° ° ° ° ° ° ° ° ° °
Garantía de transparencia	• Se adjunta un compromiso de publicación de resul- tados.	SI No No procede
Transferencia de datos fuera del centro	• Si los datos van fuera del centro se ha aportado un contrato con el encargado de tratamiento. Ej. cuando se contratan empresas para gestionar desplazamien- tos de pacientes que están participando en un estu- dio de investigación y les ceden datos identificativos. • Si se contempla la transferencia internacional de datos fuera de la Unión Europea se ha adjuntado un acuerdo que garantice que el país o la entidad de destino cum- plen con los requisitos mínimos que exige la normativa europea (p. ej. estar inscritos en el Privacy Shield).	° ° ° ° ° °
Revisión del consentimien- to informado	• Cuando proceda solicitar el consentimiento informa- do, el documento incluye los diferentes apartados exigidos por el RGPD/LOPD-GDD (ver	° ° °

	modelo anexo)	

4. Cuando se acepta la exención de consentimiento informado

		SI NO No procede
Situaciones en la que se puede aceptar la exención de consentimiento	• Cuando el interesado ha otorgado un consentimiento previo amplio, que incluya categorías relacionadas con la especialidad médica o investigadora para la que se dio el consentimiento inicial. El CEI debe verificar si el objetivo del estudio está enmarcado en los fines para los que se consintió. • Se plantea reutilizar datos obtenidos en un proyecto an- terior, para el que se dio un consentimiento concreto, para un proyecto similar (de la misma línea o ámbito de inves- tigación). El CEI debe revisar: o El objetivo del estudio: si el objetivo del proyec- to a evaluar no está enmarcado en los objetivos para los que el titular de los datos consintió, debe solicitarse un nuevo consentimiento ex- preso para el proyecto. o Que la información del nuevo uso se publique en la página web corporativa del centro donde se realice la investigación o estudio clínico. o Que se notifique a los participantes la existen- cia de esta información por medios electrónicos o Que se establezcan mecanismos para posibili- tar el rechazo a la utilización de los datos para investigación • Puede aceptarse la exención si el estudio se va a realizar con datos anonimizados o seudonimizados. En este caso el CEI debe comprobar que se dispone de las garantías adicionales establecidas por el RGPD y la LOPD-GDD.	° ° ° ° ° ° ° ° ° ° ° ° ° ° ° ° ° °

Modelo de hoja de información al paciente para realizar un estudio con datos personales

Muy Sr./Sra. nuestro:

Le proponemos participar en el estudio de investigación, de título *"xxxx"*, promovido por xx (si es un promotor externo), que va a ser realizado por xx como investigador principal. Siguiendo las guías éticas internacionales y la legislación vigente, este estudio ha sido aprobado por el comité de ética de la investigación del hospital/centro.

Antes de que usted decida si va a participar o no es importante que lea detenidamente la siguiente información, que realice todas las preguntas y solicite aclaración de todas las cuestiones que crea conveniente.

¿Tengo que participar?

La participación en el estudio es completamente voluntaria. Rechazarla no acarreará ningún deterioro en la calidad de la asistencia y el tratamiento de su enfermedad o proceso. Además, podrá retirarse en cualquier momento del estudio, sin tener que dar explicaciones y sin que ello repercuta en los cuidados médicos que recibe.

¿Objetivo del estudio?

Describir el fin y/o los fines y usos previstos de la recogida de datos personales para realizar el proyecto propuesto. Debería darse la opción de otorgar el consentimiento para determinadas áreas de investigación o partes de proyectos de investigación.

Información sobre los datos que se van a recoger

Información sobre quién va a tratar los datos; a quién los pueden ceder; quiénes son sus destinatarios o del plazo de conservación de los datos.

¿En qué consiste el estudio y cómo se va a llevar a cabo?

Debe describirse si la recogida de datos es puntual o si hay un seguimiento y la duración del mismo.

¿Qué beneficios puedo esperar por el hecho de participar en el estudio?

Explicar que en principio no se esperan beneficios. Informar, cuando corresponda, acerca de la posible generación de beneficios comerciales y/o propiedad intelectual.

¿Cómo van a ser tratados mis datos?

Sus datos personales serán registrados de forma estrictamente confidencial, conforme con el Reglamento Europeo 2016/679 de protección de datos y la Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales. En cumplimiento de esta legislación se le informa sobre el cumplimiento de las siguientes exigencias respecto al tratamiento de sus datos:

- **Identidad del responsable del tratamiento de los datos** y ante quién y cómo pueden ejercitar sus derechos (ante el investigador principal del estudio o el Delegado de Protección de Datos del centro).
- Identidad del encargado del tratamiento de los datos. Explicar quién va a tratar los datos personales.
- **Medidas de seguridad para proteger la privacidad y los riesgos para la confidencialidad.** Debe informarse sobre cómo se van a tratar los datos: anonimizados, seudonimizados o codificados, y durante cuánto tiempo se van a conservar los datos.
- Si se recogen los datos anonimizados debe informarse sobre el alcance real de los procesos de anonimización, que puede que no garanticen totalmente la irreversibilidad. Debe informarse sobre los posibles riesgos asociados a la reidentificación y la revelación de información confidencial.
- Deben explicarse las reglas de administración/gobernanza de la base de datos o formulario de recogida de datos; quién los gestiona, información sobre las medidas de seguridad del servidor en el que se van a almacenar los datos, …
- Información sobre los derechos de los titulares de los datos
- Se informa sobre el derecho de acceso, modificación, oposición y cancelación1 de los datos que van a recogerse en este estudio; derecho a limitar el tratamiento de datos que sean incorrectos o inexactos, solicitar una copia o que se trasladen a un tercero (portabilidad) los datos que se facilitan para el estudio.
- Ejemplo de párrafo: Para ejercitar sus derechos, diríjase al investigador principal del estudio *[*o al/a la **Delegado/a de Protección de Datos** del centro/institución en [dirección/link]*.] Además, podrá ampliar información en materia de protección de datos en la siguiente dirección web: xxx. Así mismo tiene derecho a dirigirse a la Agencia de Protección de Datos si no quedara satisfecho.
- Tanto el centro sanitario como el investigador son responsables respectivamente del tratamiento de sus datos y se comprometen a cumplir con la normativa de protección de datos en vigor. Los datos recogidos para el estudio estarán identificados mediante un código, de manera que no se incluya información que pueda identificarle, y sólo su médico del estudio/colaboradores podrá relacionar dichos datos con usted y con su historia clínica. Por lo tanto, su identidad no será revelada a ninguna otra persona salvo a las autoridades sanitarias, cuando así lo requieran o en casos de urgencia médica. Únicamente los comités de ética de la investigación y los representantes de la Autoridad Sanitaria en materia de inspección podrán acceder a su historia clínica para comprobar los datos personales, los procedimientos del estudio clínico y el cumplimiento de las normas de buena práctica clínica (siempre manteniendo la confidencialidad de la información).

- Usted tiene derecho a **retirar el consentimiento en cualquier momento** y la información identificable de la base de datos de salud o el formulario de recogida de datos, así como el derecho a solicitar y recibir información sobre sus datos y su uso.

Debe explicarse que si la información se anonimiza la persona no podrá saber qué se hace con su información, ni tampoco retirar su consentimiento.

En el caso de datos genéticos, debe informarse sobre los derechos amparados en la Ley 14/2007 de investigación biomédica.

Debe informarse sobre la opción futura de reutilizar los datos en estudios en finalidades relacionadas. En este caso, la información de los estudios estará disponible en la página web del centro (xxx). Además, debe solicitarse la dirección de correo electrónico para recibir la citada información.

¿Qué incomodidades o riesgos pueden suponer mi participación en el estudio?

Explicar los posibles riesgos para la confidencialidad, especialmente si los datos salen fuera del centro, describiendo los posibles riesgos asociados a la transferencia fuera de la Unión Europea, en su caso.

¿Mi participación me supondrá algún coste o compensación económica?

Explicar que la participación en el estudio no supondrá ningún coste económico, así como tampoco será recompensado económicamente por ello.

Si usted tiene alguna duda o quiere más información, no dude en consultar con el médico responsable que le está solicitando este consentimiento.

GRACIAS POR LEER ESTA INFORMACIÓN

Consentimiento informado para los participantes

Título del estudio: *"xxx"*

Investigador principal xxx

Servicio de xxx. Hospital/centro xxxx

Yo, (nombre y apellidos) ……

manifiesto que he sido informado/a del presente estudio y:

- He leído y entendido la hoja de información que se me ha entregado.
- He podido hacer preguntas sobre el estudio y sobre mis derechos.
- He recibido suficiente información sobre el estudio.
- Comprendo que mi participación es voluntaria.

- Comprendo que puedo retirarme del estudio:
- Cuando quiera.
- Sin tener que dar explicaciones.
- Sin que esto repercuta en mis cuidados médicos.
- Comprendo que mi participación en el estudio no conlleva ningún perjuicio para mi salud.
- He sido informado/a de que mis datos personales serán protegidos, que los resultados de mi evaluación personal serán estrictamente confidenciales.

ANEXO III. LISTA DE EVALUACIÓN PARA UNA INTELIGENCIA ARTIFICIAL FIABLE (GRUPO DE EXPERTOS UE 2019, VERSIÓN PILOTO)

1. Acción y supervisión humanas
2. Solidez técnica y seguridad
3. Gestión de la privacidad y de los datos
4. Transparencia
5. Diversidad, no discriminación y equidad
6. Bienestar social y ambiental
7. Rendición de cuentas

1. Acción y supervisión humanas

Derechos fundamentales:

- En aquellos casos de usos en los que puedan producirse efectos potencialmente negativos para los derechos fundamentales, ¿ha llevado usted a cabo una evaluación del impacto sobre los derechos fundamentales? ¿Ha identificado y documentado los posibles equilibrios entre los diferentes principios y derechos?
- ¿Interactúa el sistema de IA con el proceso de adopción de decisiones por parte de usuarios finales humanos (por ejemplo, con las acciones recomendadas, las decisiones que es preciso adoptar o la presentación de opciones)?
- ¿Existe en esos casos el riesgo de que el sistema de IA afecte a la autonomía humana al interferir con el proceso de adopción de decisiones del usuario final de forma imprevista?
- ¿Ha considerado usted si el sistema de IA debería informar a los usuarios de que una decisión, contenido, recomendación o resultado es fruto de una decisión algorítmica?
- En el caso de que el sistema de IA cuente con un bot de charla o un sistema conversacional, ¿son los usuarios finales humanos conocedores de que están interactuando con un agente no humano?

Acción humana:

- En el caso de que el sistema de IA se implante en el proceso de trabajo, ¿ha tenido usted en cuenta la asignación de tareas entre el sistema de IA y los trabajadores

humanos para garantizar interacciones adecuadas y una supervisión y control humanas apropiadas?

- ¿El sistema de IA mejora o aumenta las capacidades humanas?
- ¿Se han adoptado medidas para evitar que los procesos de trabajo confíen o dependan en exceso del sistema de IA?

Supervisión humana:

- ¿Ha analizado cuál sería el nivel adecuado de control humano sobre el sistema de IA específico y para el caso de uso concreto de que se trate?
- ¿Puede describir el nivel de control o implicación humana, si procede? ¿Quién es la persona que ostenta el control del sistema y cuáles son los momentos o herramientas para la intervención humana?
- ¿Ha establecido mecanismos y adoptado medidas para garantizar la posibilidad de dicho control o supervisión humanos o para asegurar que las decisiones se tomen bajo la responsabilidad exclusiva de seres humanos?
- ¿Ha adoptado alguna medida para posibilitar la realización de auditorías y para solucionar cualquier problema relacionado con la gestión de la autonomía de la IA?
- En el caso de que exista un sistema de IA (o un caso de uso) autónomo o con capacidad de autoaprendizaje, ¿ha establecido mecanismos de control y supervisión más concretos?
- ¿Qué tipo de mecanismos de detección y respuesta ha establecido para evaluar si algo puede salir mal?
- ¿Se ha asegurado de disponer de un botón de desconexión o un procedimiento que permita abortar una operación en condiciones de seguridad en caso necesario? ¿Implica ese procedimiento que se aborta el proceso en su totalidad, en parte o la delegación del control a un ser humano?

2. Solidez técnica y seguridad

Resistencia a los ataques y seguridad:

- ¿Ha evaluado las posibles formas de ataque a las que puede ser vulnerable el sistema de IA?
- En particular, ¿ha analizado los diferentes tipos y naturalezas de las vulnerabilidades, como la contaminación de los datos, la infraestructura física o los ciberataques?

- ¿Ha adoptado medidas o sistemas para garantizar la integridad del sistema de IA y su capacidad para resistir posibles ataques?
- ¿Ha evaluado el comportamiento de su sistema en situaciones o entornos imprevistos?
- ¿Ha analizado si su sistema se puede utilizar (y, en caso afirmativo, en qué medida) para diferentes fines? Si es así, ¿ha adoptado medidas adecuadas para prevenir su uso

con fines no deseados (como, por ejemplo, la no divulgación de la investigación o despliegue del sistema)?

Plan de repliegue y seguridad general:

- ¿Se ha asegurado de que su sistema cuente con un plan de repliegue suficiente en el caso de que se enfrente a algún ataque malintencionado o a otro tipo de situación inesperada (por ejemplo, procedimientos técnicos de conmutación o formulación de preguntas a un ser humano antes de continuar)?
- ¿Ha analizado el nivel de riesgo que plantea el sistema de IA en el caso de uso concreto previsto?
- ¿Ha introducido algún proceso para medir y evaluar los riesgos y la seguridad?
- ¿Ha proporcionado la información necesaria en caso de que exista algún riesgo para la integridad física de las personas?
- ¿Ha estudiado la posibilidad de contratar una póliza de seguro para hacer frente a los posibles daños que provoque el sistema de IA?
- ¿Ha identificado los riesgos potenciales para la seguridad asociados a (otros) usos previsibles de la tecnología, incluidos los usos accidentales o malintencionados? ¿Existe algún plan para mitigar o gestionar esos riesgos?

- ¿Ha evaluado si es probable que el sistema de IA cause daños a los usuarios o a terceros? En caso afirmativo, ¿ha evaluado la probabilidad, el daño potencial, el público afectado y la gravedad de tales daños?
- Si existe el riesgo de que el sistema de IA ocasione daños, ¿ha tenido en cuenta las leyes de responsabilidad civil y de protección de los consumidores? ¿Cómo?
- ¿Ha analizado los efectos potenciales o el riesgo para la seguridad del medio ambiente o de la fauna?
- ¿Ha tenido en cuenta en su análisis de riesgos si los problemas de seguridad o de la red (por ejemplo, los peligros para la ciberseguridad) plantean riesgos para la seguridad o pueden causar daños debido a un comportamiento imprevisto del sistema de IA?
- ¿Ha estimado el efecto probable de un fallo de su sistema de IA que provoque que el sistema ofrezca resultados erróneos, quede fuera de servicio o proporcione resultados socialmente inaceptables (como, por ejemplo, prácticas discriminatorias)?
- ¿Ha definido umbrales y mecanismos de gestión para los escenarios anteriores a fin de activar planes alternativos o de repliegue?
- ¿Ha definido y ensayado planes de repliegue?

Precisión

- ¿Ha evaluado qué nivel y definición de precisión se requerirá en el contexto del sistema de IA y para el caso de uso previsto?
- ¿Ha evaluado cómo se mide y garantiza la precisión?

- ¿Ha adoptado medidas para garantizar que los datos utilizados sean exhaustivos y estén actualizados?
- ¿Ha adoptado medidas para evaluar si es necesario disponer de datos adicionales, por ejemplo, para mejorar la precisión o eliminar sesgos?

- ¿Ha evaluado los daños que se ocasionarían si el sistema de IA realizara predicciones incorrectas?
- ¿Ha establecido algún mecanismo para medir si el sistema está realizando una cantidad inaceptable de predicciones erróneas?
- Si el sistema está realizando predicciones erróneas, ¿ha establecido una serie de pasos que permitan subsanar el problema?

Fiabilidad y reproducibilidad:

- ¿Ha diseñado una estrategia para supervisar y verificar que el sistema cumple los objetivos, el propósito y las aplicaciones previstas?
- ¿Ha comprobado si es necesario tener en cuenta algún contexto o condición particular para garantizar la reproducibilidad?
- ¿Ha introducido procesos o métodos de verificación para medir y garantizar los diferentes aspectos de la fiabilidad y la reproducibilidad?
- ¿Ha establecido algún proceso para describir las situaciones en las que un sistema de IA falla en determinados tipos de entornos?
- ¿Ha documentado y detallado claramente esos procesos para la verificación de la fiabilidad de los sistemas de IA?
- ¿Ha establecido algún mecanismo o comunicación para garantizar a los usuarios (finales) que el sistema de IA es fiable?

3. Gestión de la privacidad y de los datos

Respeto de la privacidad y de la protección de datos:

- Dependiendo del caso de uso, ¿ha establecido un mecanismo que permita notificar los problemas relacionados con la privacidad o la protección de datos en los procesos de recopilación de datos de los sistemas de IA (tanto con fines de formación como de funcionamiento) y su tratamiento?
- ¿Ha evaluado el tipo y alcance de los datos incluidos en sus bases de datos (por ejemplo, si estas contienen datos de carácter personal)?
- ¿Ha analizado formas de desarrollar el sistema de IA o de formar el modelo en las que no sea necesario utilizar datos personales o potencialmente sensibles (o que utilicen la mínima cantidad posible de este tipo de datos)?
- ¿Ha introducido mecanismos de aviso y control sobre los datos personales en función del caso de uso (como, por ejemplo, el consentimiento válido y la posibilidad de revocar el uso de dichos datos, cuando proceda)?
- ¿Ha tomado medidas para mejorar la privacidad, por ejemplo, a través de procesos como el encriptado, la anonimización y la agregación?
- En los casos en que exista una persona responsable de la privacidad de los datos, ¿la ha implicado desde una fase inicial del proceso?

Calidad e integridad de los datos:

- ¿Ha alineado su sistema con las normas potencialmente pertinentes (por ejemplo, ISO, IEEE) o ha adoptado protocolos generales para la gestión y gobernanza cotidianas de sus datos?
- ¿Ha establecido mecanismos de supervisión para la recopilación, almacenamiento, tratamiento y utilización de los datos?
- ¿Ha evaluado su grado de control sobre la calidad de las fuentes de datos externas utilizadas?
- ¿Ha instaurado procesos para garantizar la calidad y la integridad de sus datos? ¿Ha estudiado la posibilidad de introducir otros procesos? ¿Cómo está verificando que sus conjuntos de datos no son vulnerados ni objeto de ataques?

Acceso a los datos:

- ¿Qué protocolos, procesos y procedimientos se han seguido para gestionar y garantizar una adecuada gobernanza de los datos?
- ¿Ha evaluado quién puede acceder a los datos de los usuarios y en qué circunstancias?
- ¿Se ha asegurado de que esas personas poseen la cualificación para acceder a los datos, que se les exige acceder a ellos y que cuentan con las competencias necesarias para comprender los detalles de la política de protección de datos?
- ¿Ha asegurado la existencia de un mecanismo de supervisión que permita registrar cuándo, dónde, cómo y quién accede a los datos, y con qué propósito?

4. Transparencia

Trazabilidad:

- ¿Ha adoptado medidas que puedan garantizar la trazabilidad? Esto puede conllevar la documentación de:
    - los métodos utilizados para diseñar y desarrollar el sistema algorítmico:
        - en el caso de un sistema de IA basado en reglas, se debería documentar el método de programación o la forma en que se creó el modelo;
        - en el caso de un sistema de IA basado en el aprendizaje, se debería documentar el método de formación del algoritmo, incluidos los datos de entrada que se recopilaron y seleccionaron y la forma en que se hizo;
    - los métodos empleados para ensayar y validar el sistema algorítmico:
        - en el caso de un sistema de IA basado en reglas, se deberían documentar los escenarios
        - casos de uso utilizados para los ensayos y la validación;
        - en el caso de un modelo basado en el aprendizaje, se debería documentar la información sobre los datos utilizados para los ensayos y la validación;
    - los resultados del sistema algorítmico:
        - se deberían documentar los resultados del algoritmo o las decisiones adoptadas por este, así como otras posibles decisiones que se producirían en casos diferentes (por ejemplo, para otros subgrupos de usuarios).

Explicabilidad:

- ¿Ha evaluado en qué medida son comprensibles las decisiones y, por tanto, el resultado producido por el sistema de IA?
- ¿Se ha asegurado de que se pueda elaborar una explicación comprensible para todos los usuarios que puedan desearla sobre las razones por las que un sistema adoptó una decisión determinada que diera lugar a un resultado específico?
- ¿Ha evaluado en qué medida la decisión del sistema influye en los procesos de adopción de decisiones de la organización?
- ¿Ha evaluado por qué se desplegó ese sistema en particular en esa área concreta?
- ¿Ha evaluado el modelo de negocio del sistema (por ejemplo, de qué modo crea valor para la organización)?
- ¿Ha diseñado el sistema de IA teniendo en mente desde el principio la interpretabilidad?
- ¿Ha investigado y tratado de utilizar el modelo más sencillo e interpretable posible para la aplicación en cuestión?

- ¿Ha evaluado si puede analizar sus datos relativos a la formación y los ensayos realizados?
- ¿Puede modificar y actualizar estos datos a lo largo del tiempo?
- ¿Ha evaluado si, tras la formación y el desarrollo del modelo, tiene alguna posibilidad de examinar su interpretabilidad o si dispone de acceso al flujo de trabajo interno del modelo?

Comunicación:

- ¿Ha informado a los usuarios (finales) —mediante cláusulas de exención de responsabilidad u otros medios— de que están interactuando con un sistema de IA y no con otro ser humano? ¿Ha etiquetado su sistema de IA como tal?
- ¿Ha establecido mecanismos para informar a los usuarios de las razones y criterios subyacentes a los resultados del sistema de IA?
- ¿Se han comunicado claramente estos a los usuarios previstos?
- ¿Ha establecido procesos que tengan en cuenta las opiniones de los usuarios y que utilicen dichas opiniones para adaptar el sistema?
- ¿Ha informado sobre los riesgos potenciales o percibidos, como la posible existencia de sesgos?
- ¿Ha tenido también en cuenta, según el caso de uso, la comunicación y la transparencia hacia otras audiencias, hacia terceros o hacia el público en general?

- ¿Ha dejado claro el propósito del sistema de IA y quién o qué podrá beneficiarse del producto o servicio que ofrezca este?
- ¿Se han especificado y se ha informado claramente sobre los escenarios de utilización del producto, estudiando posibles métodos de comunicación alternativos para garantizar que dicha información sea comprensible y adecuada para los usuarios a los que se dirige?
- Según el caso de uso, ¿ha tenido en cuenta la psicología humana y sus posibles limitaciones, como el riesgo de confusión, el sesgo de confirmación o la fatiga cognitiva?
- ¿Ha comunicado con claridad las características, limitaciones y posibles carencias del sistema de IA:

    - en caso de desarrollo: a las personas encargadas de su despliegue en un producto o servicio?
    - en caso de despliegue: a los usuarios finales o consumidores?

5. Diversidad, no discriminación y equidad

Necesidad de evitar sesgos injustos:

- ¿Se ha asegurado de que exista una estrategia o un conjunto de procedimientos para evitar crear o reforzar un sesgo injusto en el sistema de IA, tanto en relación con el uso de los datos de entrada como en lo referente al diseño del algoritmo?
- ¿Ha evaluado y reconocido las posibles limitaciones que emanan de la composición de los conjuntos de datos utilizados?
- ¿Ha tenido en cuenta la diversidad y representatividad de los usuarios en los datos? ¿Ha realizado ensayos para poblaciones específicas o casos de uso problemáticos?
- ¿Ha investigado y utilizado las herramientas técnicas disponibles para mejorar su comprensión de los datos, el modelo y su rendimiento?
- ¿Ha establecido procesos para verificar la existencia de posibles sesgos y llevar a cabo un seguimiento de estos durante las fases de desarrollo, despliegue y utilización del sistema?
- Dependiendo del caso de uso, ¿se ha asegurado de introducir un mecanismo que permita a otras personas informar sobre posibles problemas relacionados con la existencia de sesgos, discriminación o un rendimiento deficiente del sistema de IA?
- ¿Ha estudiado vías y métodos de comunicación claros sobre cómo y a quién informar sobre este tipo de problemas?
- ¿Ha tenido en cuenta no solo a los usuarios (finales) sino también a otras personas que puedan verse indirectamente afectadas por el sistema de IA?
- ¿Ha evaluado si existe la posibilidad de que las decisiones varíen, aunque las condiciones no cambien?
- Si es así, ¿ha estudiado cuáles podrían ser las causas de ello?
- En caso de variabilidad, ¿ha establecido algún mecanismo de medición o evaluación del impacto potencial de dicha variabilidad sobre los derechos fundamentales?
- ¿Se ha asegurado de utilizar una definición operativa adecuada de «equidad» para aplicarla en el diseño de sistemas de IA?
- ¿Se trata de una definición de uso común? ¿Estudió otras definiciones antes de optar por la seleccionada?
- ¿Ha instaurado análisis o parámetros cuantitativos para medir y poner a prueba la definición de equidad aplicada?
- ¿Ha establecido mecanismos para garantizar la equidad en sus sistemas de IA? ¿Ha considerado otros posibles mecanismos?

Accesibilidad y diseño universal:

- ¿Se ha asegurado de que el sistema de IA se adapte a una amplia variedad de preferencias y capacidades individuales?

- ¿Ha evaluado si las personas con discapacidad, con necesidades especiales o en riesgo de exclusión pueden utilizar el sistema de IA? ¿Cómo se integró este aspecto en el sistema y cómo se verifica su funcionamiento?
- ¿Se ha asegurado de que la información sobre el sistema de IA también sea accesible para los usuarios de tecnologías asistenciales?
- ¿Implicó o consultó a esta comunidad durante la fase de desarrollo del sistema de IA?

- ¿Ha tenido en cuenta el impacto de su sistema de IA en sus usuarios potenciales?
- ¿Es el equipo involucrado en el desarrollo del sistema de IA representativo de la audiencia a la que va dirigido? ¿Es representativo de la población en general y tiene también en cuenta a otros grupos que pudieran verse afectados de manera tangencial por el sistema?
- ¿Ha evaluado la posibilidad de que haya personas o grupos que puedan verse afectados de forma desproporcionada por las implicaciones negativas del sistema?
- ¿Ha recabado la opinión de otros equipos o grupos representativos de diferentes contextos y experiencias?

Participación de las partes interesadas:

- ¿Ha estudiado la posibilidad de introducir algún mecanismo para incorporar la participación de diferentes partes interesadas en el desarrollo y la utilización del sistema de IA?
- ¿Ha allanado el camino para la introducción del sistema de IA en su organización, informando e implicando previamente a los trabajadores afectados y sus representantes?

6. Bienestar social y ambiental

Una IA sostenible y respetuosa con el medio ambiente:

- ¿Ha establecido mecanismos para medir el impacto ambiental del desarrollo, despliegue y utilización del sistema de IA (por ejemplo, energía consumida por cada centro de datos, tipo de energía utilizada por los centros de datos, etc.)?
- ¿Se ha asegurado de introducir medidas para reducir el impacto ambiental de su sistema de IA a lo largo de todo su ciclo de vida?

Impacto social:

- En el caso de que el sistema de IA interactúe directamente con seres humanos:
- ¿Ha evaluado si el sistema de IA alienta a los humanos a establecer un vínculo y desarrollar la empatía con el sistema?

- ¿Se ha asegurado de que el sistema indique claramente que su interacción social es simulada y que no tiene capacidad para «entender» ni «sentir»?
- ¿Se ha asegurado de que se entiendan correctamente los efectos sociales del sistema de IA? Por ejemplo, ¿ha evaluado si existe un riesgo de pérdida de puestos de trabajo o de descualificación de la mano de obra? ¿Qué pasos se han dado para contrarrestar esos riesgos?

Sociedad y democracia:

- ¿Ha evaluado el impacto social global asociado al uso del sistema de IA más allá del que tenga sobre el usuario (final), como, por ejemplo, las partes interesadas que pueden verse indirectamente afectadas por dicho sistema?

7. Rendición de cuentas

Auditabilidad:

- ¿Ha establecido mecanismos para facilitar la auditabilidad del sistema por parte de agentes internos o independientes (garantizando, por ejemplo, la trazabilidad y registro de los procesos y resultados del sistema de IA)?

Minimización de efectos negativos y notificación de estos:

- ¿Ha llevado a cabo una evaluación de riesgos o de impacto del sistema de IA que tenga en cuenta a las diferentes partes interesadas que se vean afectadas por este de forma directa o indirecta?
- ¿Ha establecido marcos de formación y educación para el desarrollo de prácticas de rendición de cuentas?
- ¿Qué trabajadores o partes del equipo están implicados en ello? ¿Trasciende la fase de desarrollo?
- ¿Se explica también en esa formación el posible marco jurídico aplicable al sistema de IA?
- ¿Ha considerado la posibilidad de crear una «junta de revisión ética de la IA» u otro mecanismo similar para debatir sobre las prácticas éticas y de rendición de cuentas en general, incluidas las posibles «zonas grises»?
- Además de las iniciativas o marcos internos para supervisar la ética y la rendición de cuentas, ¿se cuenta con algún tipo de orientación externa o se han establecido también procesos de auditoría?
- ¿Existe algún proceso para que los trabajadores o agentes externos (por ejemplo, proveedores, consumidores, distribuidores/vendedores) informen sobre posibles vulnerabilidades, riesgos o sesgos en el sistema de IA o su aplicación?

Documentación de los equilibrios alcanzados:

- ¿Se ha establecido algún mecanismo para identificar los intereses y valores que implica el sistema de IA y los posibles equilibrios entre ellos?

- ¿Qué procesos ha seguido para decidir sobre los equilibrios necesarios? ¿Se ha asegurado de documentar la decisión sobre la búsqueda de dichos equilibrios?

Capacidad de obtener compensación:

- ¿Ha establecido un conjunto de mecanismos adecuado que permita obtener compensación en el caso de que se produzca cualquier daño o efecto adverso?
- ¿Se han instaurado mecanismos para proporcionar información a usuarios (finales) y a terceros sobre las oportunidades de obtener compensación?

ANEXO IV. "CHECK LIST" DE LOS CONTROLES A AUDITAR

En la Guía Requisitos para auditorías de enero 2021 de la AEPD se determinan los objetivos y a partir de ellos se detalla concretamente el check list de los controles a realizar, **aproximadamente unos 160**. En cualquier caso (ob. Cit. p. 13) se recuerda que "no implica la obligación de aplicar sistemáticamente todos y cada uno de ellos, sino que hay que seleccionar, de forma racional, aquellos relevantes para cumplir con el objeto y el alcance definidos para la auditoría".

A. Identificación y transparencia del componente

- Objetivo: Inventario del componente IA auditado
- Objetivo: Identificación de responsabilidades
- Objetivo: Transparencia

B. Propósito del componente IA

- Objetivo: Identificación de las finalidades y usos previstos
- Objetivo: Identificación del contexto de uso del componente IA
- Objetivo: Análisis de la proporcionalidad y necesidad
- Objetivo: Determinación de los destinatarios de los datos
- Objetivo: Limitación de la conservación de datos
- Objetivo: Análisis de las categorías de interesados

C. Fundamentos del componente IA

- Objetivo: Identificación de la política de desarrollo del componente IA
- Objetivo: Implicación del DPD
- Objetivo: Adecuación de los modelos teóricos base
- Objetivo: Adecuación del marco metodológico
- Objetivo: Identificación de la arquitectura básica del componente

D. Gestión de los datos

- Objetivo: Aseguramiento de la calidad de los datos
- Objetivo: Determinación del origen de las fuentes de datos
- Objetivo: Preparación de los datos personales
- Objetivo: Control del sesgo

E. Verificación y validación

- Objetivo: Adecuación del proceso de verificación y validación del componente IA
- Objetivo: Verificación y Validación del componente IA
- Objetivo: Rendimiento

- Objetivo: Coherencia
- Objetivo: Estabilidad y robustez
- Objetivo: Trazabilidad
- Objetivo: Seguridad

ANEXO V. PARLAMENTO EUROPEO. CÓDIGOS DE CONDUCTA Y LICENCIAS DE DISEÑADORES Y USUARIOS ROBÓTICA

Código de conducta ética para los ingenieros en robótica

Parlamento Europeo 2017. Anexo.

PREÁMBULO

El código de conducta invita a todos los investigadores y diseñadores a actuar de forma responsable y con la máxima consideración a la necesidad de respetar la dignidad, intimidad y la seguridad de las personas.

El código pide una estrecha colaboración entre todas las disciplinas a fin de garantizar que se lleve a cabo la investigación en robótica en la Unión de un modo seguro, ético y eficaz.

El código de conducta cubre todas las actividades de investigación y desarrollo en el campo de la robótica.

El código de conducta es voluntario y ofrece un conjunto de principios generales y directrices para las medidas que adopten todas las partes interesadas.

Se invita a los organismos de financiación en materia de robótica, los centros de investigación, los investigadores y los comités de ética a que examinen desde las primeras etapas, las consecuencias futuras de las tecnologías u objetos que se investigan y de crear una cultura de la responsabilidad para hacer frente a los retos y oportunidades que puedan plantearse en el futuro.

Los organismos públicos y privados de financiación de la investigación en el ámbito de la robótica deberían exigir la realización y presentación de una evaluación del riesgo para cada propuesta de financiación de la investigación en la materia. Un código de estas características debería considerar que la responsabilidad incumbe a los seres humanos, no a los robots.

Los investigadores en el campo de la robótica deberían comprometerse a adoptar una conducta estricta en materia de ética y de deontología, así como a respetar los siguientes principios:

Beneficencia — los robots deben actuar en beneficio del hombre;

Principio de no perjuicio o maleficencia — la doctrina de «primero, no hacer daño», en virtud del cual los robots no deberían perjudicar a las personas;

Autonomía — la capacidad de tomar una decisión con conocimiento de causa e independiente sobre los términos de interacción con los robots;

Justicia — la distribución justa de los beneficios asociados a la robótica y la asequibilidad de los robots utilizados en el ámbito de la asistencia sanitaria a domicilio y de los cuidados sanitarios en particular.

Derechos fundamentales

Las actividades de investigación en materia de robótica deben respetar los derechos fundamentales; y por su parte, las actividades de concepción, ejecución, difusión y explotación, por su parte, han de estar al servicio del bienestar y la autodeterminación de las personas y de la sociedad en general. La dignidad y la autonomía humanas — tanto físicas como psicológicas — siempre tienen que respetarse.

Precaución

Las actividades de investigación en el ámbito de la robótica deben llevarse a cabo de conformidad con el principio de precaución, anticipándose a los posibles impactos de sus resultados sobre la seguridad y adoptando las precauciones debidas, en función del nivel de protección, al tiempo que se fomenta el progreso en beneficio de la sociedad y del medio ambiente.

Participación

Los ingenieros en robótica garantizan la transparencia y el respeto al derecho legítimo de acceso a la información de todas las partes interesadas. La integración permite la participación en los procesos de toma de decisiones de todas las partes interesadas o afectadas por las actividades de investigación en el ámbito de la robótica.

Rendición de cuentas

Los ingenieros en robótica deben rendir cuentas de las consecuencias sociales y medioambientales y el impacto sobre la salud humana que la robótica puede conllevar para las generaciones presentes y futuras.

Seguridad

Los diseñadores de robots han de tener en cuenta y respetar la integridad física, la seguridad, la salud y los derechos de las personas. Un ingeniero en robótica debe preservar el bienestar sin dejar de respetar los derechos humanos, y divulgar con prontitud los factores susceptibles de poner en peligro a la población o al medio ambiente.

Reversibilidad

La reversibilidad, que es una condición necesaria de la posibilidad de control, es un concepto fundamental en la programación de robots para que se comporten de manera segura y fiable. Un modelo de reversibilidad indica al robot qué acciones son reversibles y, en su caso, el modo de invertirlas. La posibilidad de deshacer la última acción o secuencia de acciones permite al usuario anular las acciones no deseadas y volver a la fase «buena» de su trabajo.

Privacidad

El derecho a la intimidad debe siempre respetarse. Un ingeniero en robótica debe garantizar que la información privada se conservará en total seguridad y solo se utilizará de forma adecuada. Por otra parte, el ingeniero en robótica ha de garantizar que los individuos no son personalmente identificables, salvo en circunstancias excepcionales, y únicamente en caso de consentimiento claro, consciente e inequívoco. El consentimiento consciente de la persona tiene que solicitarse y recabarse con anterioridad a cualquier interacción hombre-máquina. A tal efecto, los diseñadores en robótica tienen la responsabilidad de desarrollar y aplicar procedimientos para garantizar el consentimiento válido, la confidencialidad, el anonimato, el trato justo y el respecto de la legalidad. Los diseñadores llevarán a cabo todas las solicitudes de destrucción de los datos relacionados y de eliminación de las bases de datos.

Maximizar beneficios y reducir al mínimo los daños

Los investigadores deben intentar maximizar los beneficios de su actividad en todas las fases, desde su concepción hasta su difusión. Es conveniente evitar cualquier daño a los participantes o a los seres humanos que participen en los experimentos, ensayos o estudios en el ámbito de la investigación. En caso de aparición de riesgos inevitables que formen parte de un elemento integrante de la investigación, sería necesario llevar a cabo una evaluación sólida de los riesgos, desarrollar protocolos de gestión y adecuarse a los mismos. Normalmente, los riesgos a un daño no deberían ser superior a los existentes en la vida cotidiana, es decir, las personas no han de estar expuestas a riesgos mayores o adicionales a aquellos a los que están expuestos en su vida cotidiana. La explotación de un sistema de robótica debería basarse siempre en una profunda evaluación de los riesgos, y reposar en los principios de proporcionalidad y de precaución.

Código deontológico para los comités de ética de la investigación

Principios

Independencia

El proceso de revisión ética ha de ser independiente de la propia investigación. Este principio pone de relieve la necesidad de evitar conflictos de intereses entre los investigadores y aquellos encargados de revisar el protocolo ético, y entre los revisores y las estructuras de gobernanza organizativa.

Competencia

Sería conveniente que el proceso de revisión ética fuera efectuado por revisores con experiencia adecuada, teniendo en cuenta la necesidad de un examen cuidadoso de la diversidad en la composición y en la formación específica en materia de ética de los comités de ética de la investigación.

Transparencia y obligación de rendir cuentas

El proceso de revisión debería ser responsable y en condiciones de ser objeto de control. Los comités de ética de la investigación regionales deben ser conscientes de sus responsabilidades y estar adecuadamente ubicados dentro de estructuras organizativas

que les doten de transparencia operativa y de procedimientos destinados a conservar y revisar las normas.

La función de un comité de ética de la investigación

Normalmente, los comités de ética de la investigación son responsables de revisar toda investigación en la que intervienen participantes humanos realizada por persona empleadas en o por la institución en cuestión; de garantizar que la revisión ética es independiente, competente y oportuna; de proteger la dignidad, los derechos y el bienestar de los sujetos participantes de la investigación; de velar por la seguridad de los investigadores; de tener en cuenta los intereses legítimos de las demás partes interesadas; de hacer juicios razonados del mérito científico de las propuestas; de formular recomendaciones con conocimiento de causa al investigador si la propuesta es considerada insuficiente en determinados aspectos.

Constitución de un Comité de Ética de la Investigación

Un Comité de Ética de la Investigación debería tener normalmente un carácter multidisciplinar: incluir a hombres y mujeres, estar constituido por miembros con una amplia experiencia y conocimientos en el ámbito de la investigación en robótica. El mecanismo de designación debería velar por que los miembros del comité garanticen un equilibrio adecuado entre conocimientos científicos, formación filosófica, ética o jurídica, así como diferentes puntos de vista. Además, debería contar con al menos un miembro con conocimientos especializados en materia de ética y con usuarios de servicios especializados de salud, educación o servicios sociales cuando dichos ámbitos figuren dentro de las actividades de investigación, así como con miembros que dispongan de conocimientos metodológicos específicos relacionados con la investigación que evalúen, de tal forma que se eviten los conflictos de intereses.

Control

Sería conveniente que todos los organismos de investigación establecieran procedimientos adecuados para supervisar la ejecución de la investigación que haya recibido el visto bueno en materia de ética hasta la finalización del mismo, y garantizar una revisión continua en el supuesto de que el diseño de la investigación prevea posibles cambios a lo largo del tiempo que debieran tratarse. Los controles deberían ser proporcionados a la naturaleza y a la intensidad del riesgo vinculado con la investigación. Cuando un comité de ética de la investigación considere que un informe de seguimiento plantea importantes dudas sobre la conducta ética del estudio, deberá solicitar un detalle pormenorizado y exhaustivo de la investigación con vistas a efectuar un examen ético. Cuando considere que un estudio se está llevando a cabo de una forma contraria a la ética, debería plantearse la retirada de su aprobación y suspenderse o interrumpirse la investigación.

Licencia para los diseñadores

- Los diseñadores deberán tener en cuenta los valores europeos de dignidad, autonomía y autodeterminación, libertad y justicia, antes, durante y después del proceso de concepción, desarrollo y de aplicación de esas tecnologías, incluida la necesidad de no perjudicar, herir, engañar o explorar a los usuarios (vulnerables).

- Los diseñadores deberán introducir principios de diseño de sistemas fiables en todos los aspectos del funcionamiento de un robot, tanto para la concepción del material y de programas informáticos, como para el tratamiento de datos dentro o fuera de la plataforma a efectos de seguridad.
- Los diseñadores deberán introducir dispositivos concebidos para asegurar que las informaciones privadas se conservan con total seguridad y solo se utilizan de manera adecuada.
- Los diseñadores deberán integrar mecanismos de salida evidentes (teclas de interrupción de urgencia) que deberán ser coherentes con los objetivos de diseño razonables.
- Los diseñadores deberán garantizar que un robot funciona de modo conforme a los principios éticos y jurídicos a nivel local, nacional e internacional.
- Los diseñadores deberán asegurarse de que las etapas de toma de decisión del robot puedan ser objeto de reconstrucción y trazabilidad.
- Los diseñadores deberán asegurarse de que es conveniente una transparencia máxima en la programación de los sistemas robóticos, así como la previsibilidad del comportamiento de los robots.
- Los diseñadores deberán analizar la previsibilidad de un sistema humano-robot teniendo en cuenta la incertidumbre en la interpretación y en la acción, así como los posibles fallos de los robots o del hombre.
- Los diseñadores deberán desarrollar instrumentos de rastreo en la fase de concepción del robot. Estos instrumentos permitirán tener en cuenta y explicar los comportamientos de los robots, aunque sea de forma limitada, en los distintos niveles previstos para los expertos, los operadores y los usuarios.
- Los diseñadores deberán elaborar protocolos de concepción y evaluación, y colaborar con los usuarios y las partes interesadas potenciales para evaluar las ventajas y los riesgos de la robótica, incluido a nivel cognitivo, psicológico y medioambiental.
- Los diseñadores deberán asegurarse de que los robots son identificables como tales al relacionarse con seres humanos.
- Los diseñadores deberán salvaguardar la seguridad y la salud de las personas que interactúan y entran en contacto con los robots, teniendo en cuenta que estos, como productos, deberán elaborarse utilizando procesos que garantizan su seguridad y protección. Un ingeniero en robótica ha de preservar el bienestar humano, al tiempo que respeta los derechos humanos, y no podrá accionar un robot sin garantizar la seguridad, la eficacia y la reversibilidad del funcionamiento del sistema.
- Los diseñadores deberán obtener el dictamen favorable de un comité de ética de la investigación antes de probar un robot en un entorno real o implicando a seres humanos en los procedimientos de concepción y desarrollo.

Licencia para los usuarios

- Los usuarios estarán autorizados a hacer uso de un robot sin miedo de perjuicio físico o psicológico.

- Los usuarios deben tener derecho a esperar que un robot efectúe las tareas para las que haya sido expresamente concebido.
- Los usuarios deben ser consciente de que los robots pueden tener límites de percepción, límites cognitivos y límites de accionamiento.
- Los usuarios deberán respetar la fragilidad humana, tanto física como psicológica, así como las necesidades emocionales de los seres humanos.
- Los usuarios deben tener en cuenta el derecho a la vida privada de las personas, incluida la desactivación de videomonitores durante procedimientos íntimos.
- Los usuarios no están autorizados a recoger, utilizar o divulgar información personal sin el consentimiento explícito de la persona concernida.
- Los usuarios no están autorizados a utilizar un robot de modo contrario a los principios y normas éticas o jurídicas.
- Los usuarios no están autorizados a modificar los robots para utilizarlos como armas.


ITI
INVESTIGATE
TO INNOVATE