UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Facultad de Administración y Dirección de Empresas /UPV

UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Facultad de Administración y Dirección de Empresas

Condiciones legales para el ejercicio de derechos en relación con el tratamiento de datos personales de las personas físicas

Trabajo Fin de Grado

Grado en Gestión y Administración Pública

AUTOR/A: Huerta Salvador, Alba

Tutor/a: Amat Llombart, Pablo

CURSO ACADÉMICO: 2023/2024

CONDICIONES LEGALES PARA EL EJERCICIO DE DERECHOS EN RELACIÓN CON EL TRATAMIENTO DE DATOS PERSONALES DE LAS PERSONAS FÍSICAS

Facultad de Administración y Dirección de Empresas
Grado en Gestión y Administración Pública
Curso 2023-2024

Autora: Alba Huerta Salvador
Tutor(a): Pablo Amat Llombart

RESUMEN

El presente trabajo tiene como objetivo general analizar y evaluar el marco legal y los derechos de privacidad en relación con el tratamiento de datos personales desde una perspectiva europea y española. En concreto, se abordará el estudio de las garantías legales existentes en cuanto al ejercicio de tales derechos.

Como referencia normativa el trabajo se fundamenta, a nivel europeo, en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Y a nivel nacional en la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales.

Asimismo, este TFG tiene como objetivo específico profundizar en el estudio de los derechos ARCO (Acceso, Rectificación, Cancelación y Oposición), entre otros. Estos derechos se reconocen a las personas físicas para ejercer el control sobre sus datos personales.

PALABRAS CLAVE:

Protección de datos, derechos personales, personas físicas, garantías legales y derechos ARCO.

ABSTRACT

This assignment aims to analyze and assess the legal framework and privacy rights concerning the processing of personal data from both a European and Spanish perspective. Specifically, it will address the study of existing legal guarantees regarding the exercise of such rights.

As a normative reference, this work is grounded, at the European level, in Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016, regarding the protection of individuals concerning the processing of personal data and the free movement of such data. At the national level, it is based on Organic Law 3/2018, of December 5, on the protection of personal data and guarantee of digital rights.

Additionally, this thesis has the specific objective of delving into the study of ARCO rights (Access, Rectification, Cancellation, and Opposition), among others. These rights are recognized for individuals to exert control over their personal data.

KEYWORDS**:**

Data protection, personal rights, natural persons, legal guarantees and ARCO rights.

RESUM

El present treball té com a objectiu general analitzar i avaluar el marc legal i els drets de privacitat en relació amb el tractament de dades personals des d'una perspectiva europea i espanyola. En concret, s'abordarà l'estudi de les garanties legals existents quant a l'exercici de tals drets.

Com a referència normativa el treball es fonamenta, a nivell europeu, en el Reglament (UE) 2016/679 del Parlament Europeu i del Consell, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'estes dades. I a nivell nacional en la Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals.

Així mateix, este TFG té com a objectiu específic aprofundir en l'estudi dels drets ARC (Accés, Rectificació, Cancel·lació i Oposició), entre altres. Estos drets es reconeixen a les persones físiques per a exercir el control sobre les seues dades personals.

PARAULES CLAU:

Protecció de dades, drets personals, persones físiques, garanties legals i drets ARC.

LISTA DE ABREVIATURAS

AEPD: Agencia Española de Protección de Datos

ARCO: Acceso, Rectificación, Cancelación, Oposición.

CE: Constitución Española

LOPD: Ley 3/2018 de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales

LORTAD: Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal

ODS: Objetivos de Desarrollo sostenible

RAT: Registro de Actividades de Tratamiento

RGPD: Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos.

UE: Unión Europea

ÍNDICE DE CONTENIDO

1. INTRODUCCIÓN

1.1. JUSTIFICACIÓN

La protección de datos personales y garantía de derechos digitales es un tema de plena actualidad, especialmente por el desarrollo tecnológico y el proceso de digitalización iniciado en décadas anteriores. La incorporación al ámbito privado, público y laboral de equipos informáticos, elementos de almacenamiento de datos, sistemas avanzados de comunicación y, principalmente el uso de Internet como conjunto de redes interconectadas a nivel mundial, ha propiciado unos riesgos que la sociedad ha ido aceptando.

Este vertiginoso proceso de digitalización al que nos hemos sometido ha dado origen a una organización social en la que los intercambios diarios digitales están conformados por Tecnologías de la Información y Comunicación (TIC), sistemas de procesamiento y gestión de la información y nuevos sistemas de comunicación, interconexión y almacenamiento, etc. que ha conformado una sociedad digital en la que constantemente se recopilan, utilizan y distribuyen datos personales. Y se ha visto la necesidad de que sea la ciudadanía la que debe poder decidir libremente sobre la base del consentimiento cómo desea que se utilicen sus propios datos para evitar abusos, teniendo la garantía de que sus datos se usarán para fines concretos y legítimos y sobre la base del consentimiento o en virtud de la seguridad jurídica que le ofrece la normativa legal aplicable. Toda persona debe tener derecho a acceder a los datos que le conciernen y a obtener su rectificación o revocación del consentimiento sobre su uso.

1.2. OBJETO Y OBJETIVOS DEL TFG

Este TFG tiene por objeto analizar la normativa aplicable sobre la protección de datos, su evolución histórica, objetivos y aplicación, desde la perspectiva nacional y europea.

1.2.1. Ámbito nacional

La protección de los datos personales es un derecho fundamental protegido en la Constitución española de 1978. En su artículo 18, apartado 1 “se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen”. Asimismo, en el apartado 4 del citado artículo, se establece que “la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.

Los derechos al honor, la intimidad personal y familiar y a la propia imagen, son derechos fundamentales que forman parte de los bienes de la personalidad que se vinculan a la vida privada de las personas físicas.

El derecho a la intimidad está en estrecha conexión con el derecho a la protección de datos personales ya que ambos tienen como objeto garantizar que el individuo pueda desarrollarse libremente; de forma que la protección de datos de carácter personal se encuentra vinculada con la garantía constitucional a la tutela de los derechos al honor, a la intimidad personal y a la propia imagen (art 18.1 y 18.4 CE).

Así el artículo 53 de la CE ofrece una doble garantía constitucional a la tutela de las libertades y de los derechos fundamentales reconocidos en el Capítulo I del Título I, ya que establece una reserva de ley que implica que la regulación de dicha materia ha de hacerse por ley, en cuanto a su contenido esencial, la regulación de su ejercicio, que podrá ser objeto de recurso de inconstitucionalidad ante el Tribunal Constitucional. Asimismo, cualquier ciudadano podrá recabar la tutela de las libertades y derechos reconocidos en el artículo 14 y la Sección primera del Capítulo segundo, entre los que se incluye el artículo 18.1 y 18.4, ante los Tribunales ordinarios por un procedimiento basado en los principios de preferencia y sumariedad y, en su caso, a través del recurso de amparo ante el Tribunal Constitucional.

La protección de datos personales se erige como un pilar fundamental en el resguardo del honor, la intimidad y los derechos de los ciudadanos; así lo plasman las siguientes sentencias del Tribunal Constitucional:

- La **Sentencia 94/1998, de 4 de mayo de 1998, del Tribunal Constitucional**, establece de manera inequívoca que este derecho fundamental es esencial para otorgar a las personas el control absoluto sobre sus datos, evitando así su uso indebido o cualquier actividad que pueda menoscabar su dignidad o derechos.
- Y la **Sentencia 292/2000, de 30 de noviembre de 2000**, enfatiza que el derecho a la protección de datos es independiente y autónomo, otorgando a los individuos un poder de disposición sobre sus datos personales. Este poder permite decidir quién puede acceder a dichos datos, ya sea el Estado o un particular, así como oponerse a su uso si así lo desean.

En el ámbito legislativo nacional, la materialización y desarrollo de este derecho se realizó en el año 1992 con la aprobación de la primera ley dedicada a la protección de datos personales: la Ley Orgánica 5/1992, de 29 de octubre de Regulación del Tratamiento

Automatizado de los Datos de Carácter Personal, conocida como LORTAD. Posteriormente, esta ley fue sustituida por la Ley Orgánica 15/1999, de protección de datos personales (LOPD), con el objetivo de adaptar la normativa española a la Directiva 95/46/CE del Parlamento Europeo y del Consejo.

Actualmente la normativa vigente en el ámbito de la protección de datos de carácter personal se compone del:

- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 (RGPD), y de la
- Ley Orgánica 3/2018, de 5 de diciembre de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPD)

1.2.2. Ámbito europeo

A nivel europeo, la protección de los datos personales es un derecho fundamental consagrado en la Carta de los Derechos Fundamentales de la Unión Europea y en el Tratado de Funcionamiento de la Unión Europea. En la Carta se recogen todos los derechos individuales, civiles, políticos, económicos y sociales que disfrutan todas las personas en la Unión Europea y, concretamente el artículo 8 establece que “toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan” y se dispone lo mismo en el artículo 16, párrafo 1 del Tratado de Funcionamiento de la Unión Europea. Cualquier persona que resida en la Unión, cuyos datos personales sean tratados en la Unión, o cuando dicho tratamiento se refiera a la oferta de bienes o servicios a dicha persona en la Unión o al control de su conducta en la Unión, está protegida por el marco jurídico adoptado por la Unión de conformidad con el artículo 8 de la Carta y con el artículo 16 del Tratado de Funcionamiento de la Unión Europea.

Por otra parte, la Directiva 95/46/CE, buscaba armonizar las normativas de protección de datos entre los Estados miembros de la Unión Europea, garantizando así la libre circulación de los datos dentro del mercado común. Fue derogada por el vigente:

- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos).

El paquete de medidas sobre protección de datos, adoptado en mayo de 2016, busca preparar a Europa para la era digital. Más del 90 % de los europeos quieren tener el mismo

derecho a la protección de sus datos en toda la UE y con independencia del lugar donde se realice su tratamiento

Es importante destacar que estas regulaciones no solo procuran proteger los datos dentro del ámbito europeo, sino que también establecen salvaguardas para su tratamiento en caso de transferencias internacionales, asegurando que los estándares de protección se mantengan independientemente del país de destino. Además de estas disposiciones, la evolución tecnológica y el aumento del uso de datos en la sociedad digital han generado la necesidad de reformas y actualizaciones constantes en la legislación sobre protección de datos. En este sentido, la entrada en vigor del Reglamento (UE) 2018/1725 muestra un avance significativo en la regulación de la privacidad y la protección de datos en Europa. Este reglamento refuerza y amplía los derechos de los ciudadanos en relación con sus datos personales, imponiendo obligaciones más estrictas a las organizaciones que los tratan.

El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, (Reglamento general de protección de datos, RGPD) y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), establecen el marco legal de referencia que desarrolla el derecho fundamental a la protección de datos personales. Queda derogada la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, sin perjuicio de lo previsto en la disposición adicional decimocuarta de la LOPDGDD, y siguen vigentes las disposiciones de su Reglamento, aprobado por Real Decreto 1720/2007, de 21 de diciembre, que no contradigan, se opongan, o resulten incompatibles con lo dispuesto en el RGPD y la LOPDGDD.

Para el tratamiento de datos personales relativos a condenas e infracciones penales, la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales constituye la norma de referencia por la que se rige el tratamiento de este tipo de datos. Dicha Ley Orgánica traspone a nuestro ordenamiento jurídico la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 relativa a esta misma materia.

1.3. METODOLOGÍA

Como se ha indicado anteriormente, en este trabajo se va a realizar un análisis de la normativa aplicable sobre la protección de datos, su evolución histórica, objetivos y aplicación, desde la perspectiva nacional y europea. Entrando a detallar los derechos que tienen las personas físicas en relación con la protección de sus datos personales, los cuales están diseñados para garantizar su privacidad y el control de su información, uso y difusión.

Se aborda el estudio de las autoridades administrativas independientes, estatales y autonómicas, con personalidad jurídica y plena capacidad, encargadas de velar por el cumplimiento de la normativa sobre protección de datos y que constituyen la "autoridad de control", que el RGPD determinaba que debían establecer los Estados miembros de la UE a efectos de supervisar su aplicación con la finalidad de proteger los derechos de las personas físicas.

Para realizar esta tarea se ha accedido a diferentes fuentes de datos, principalmente fuentes secundarias: recopilación legislativa a través del Boletín Oficial del Estado (BOE), el Diario Oficial de la Unión Europea (DOUE), páginas estales y autonómicas y de organizaciones especializadas en el tema, etc. Respecto a fuentes primarias consultadas han sido entrevistadas personas afectadas por la vulneración de sus derechos de protección de datos personales.

Otra fuente secundaria consultada han sido las memorias anuales que redacta la Agencia Española de Protección de Datos en las que analizan las tendencias legislativas, jurisprudenciales y doctrinales de otros países y hacen una valoración de los problemas de la protección de datos.

1.4 RELACIÓN DEL TFG CON LAS ODS

La relación de este TFG con los ODS[1] se concreta en los objetivos 9, 10, 16 y 17. El objetivo 9 hace referencia a la industria, innovación e infraestructura, que lo relacionamos con la promoción de condiciones legales adecuadas en el ámbito del tratamiento de datos

[1] Disponible en: https://www.un.org/sustainabledevelopment/es/objetivos-de-desarrollo-sostenible/

fomentando así al desarrollo de infraestructuras digitales sólidas que garanticen los derechos de privacidad.

El objetivo 10 se refiere a la "Reducción de las Desigualdades" y hace referencia en cuanto a la implementación de condiciones legales claras y equitativas en el tratamiento de datos. Un marco legal que garantiza que todos los individuos, independientemente de su origen o posición social, tengan igualdad de derechos en cuanto a la privacidad y protección de datos.

Seguidamente, el objetivo 16 "Paz, Justicia e Instituciones Sólidas", está relacionado con la protección de datos personales ya que es esencial para promover sociedades pacíficas e inclusivas. Garantizar condiciones legales sólidas en el tratamiento de datos es fundamental para garantizar la privacidad y seguridad de los individuos, un aspecto clave para construir sociedades justas y pacíficas.

Por último, el objetivo 17 es el referido a las "Alianzas para lograr los objetivos", relacionado con la protección de datos personales requiere colaboración y alianzas entre diferentes actores, como gobiernos, empresas y sociedad civil. Establecer condiciones legales efectivas fomenta estas alianzas y contribuye a la consecución de objetivos más amplios, promoviendo una gestión ética de la información personal.

En conjunto, este TFG contribuye a avanzar hacia un entorno más justo, equitativo, innovador y colaborativo, alineándose con varios ODS y promoviendo prácticas éticas en el tratamiento de datos personales.

1.5 RELACIÓN DEL TFG CON LAS ASIGNATURAS DE GAP

El presente trabajo se relaciona con las siguientes asignaturas estudiadas a lo largo de la carrera:

- Derecho Constitucional y Fundamentos de derecho y Principios constitucionales: Inmersión en el estudio y comprensión de los derechos fundamentales y libertades públicas protegidos por la Constitución Española.
- Introducción a la Ciencia Política: Conocimientos adquiridos sobre procesos de elaboración y aprobación de leyes, la organización política basada en los Estados y las consecuencias políticas y normativas consecuencia de la globalización de la sociedad.

- Derecho Administrativo: Aproximación al acto administrativo y al procedimiento administrativo común español, especialmente en referencia a los procedimientos administrativos iniciados por las reclamaciones presentadas por los interesados ante autoridades públicas independientes encargadas de proteger a la ciudadanía y velar por el cumplimiento normativo.
- Estructuras administrativas: aproximación al régimen jurídico de las Administraciones Públicas y a los organismos públicos y entidades de derecho público vinculados o dependientes ellas; en especial la Administración General del Estado y las Administraciones de las Comunidades Autónomas. Así como a determinadas Instituciones de la Unión Europea
- Informes y Dictámenes Administrativos: Elaboración de textos administrativos y comprensión de documentos institucionales (memorias, informes, dictámenes, planes estratégicos, etc.)
- Gestión Jurídico Administrativa: Realizar una correcta comprensión e interpretación de los textos normativos, españoles y europeos.
- Metodología del TFG: Realizar la maquetación y organización en la preparación del presente TFG.
- Consumidores, Ciudadanos y Seguridad Pública: aproximación a la normativa jurídica que regula las relaciones de los consumidores y usuarios con la Administración Pública y las empresas privadas y nociones del marco normativo básico de seguridad pública. Así como la aproximación a los derechos, libertades y obligaciones que se ejercitan en el ámbito jurídico público y privado.

1.6 ESTRUCTURA DEL TFG

Este trabajo se configura por:

- El marco normativo vigente sobre la protección de datos personales, libre circulación de datos y garantía de los derechos digitales, español y europeo.
- El marco teórico y conceptual de los datos personales, como objeto de protección; y del individuo como sujeto de la protección legal.
- El marco teórico sobre las figuras clave para el cumplimiento de la normativa de protección de datos.
- Clasificación y análisis de los derechos que tienen las personas físicas en relación con la protección de sus datos personales, recogidos en la normativa vigente.

- El marco teórico sobre las autoridades administrativas independientes, estatales y autonómicas, que son la “autoridad de control” encargadas de velar por el cumplimiento de la normativa sobre protección de datos.
- Finalmente, se incluyen las conclusiones y referencias bibliográficas.

2. MARCO NORMATIVO

2.1 ANTECEDENTES SOBRE PROTECCIÓN DE DATOS PERSONALES, LIBRE CIRCULACIÓN DE DATOS Y GARANTÍA DE LOS DERECHOS DIGITALES

Los antecedentes normativos sobre la protección de las personas físicas en relación con el tratamiento de datos personales los encontramos en la propia Constitución española, ya que en su artículo 18.4 reconoce el derecho fundamental a la protección de datos personales y lo protege al establecer que «la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos».

Los derechos al honor, la intimidad personal y familiar y a la propia imagen, son derechos fundamentales que forman parte de los bienes de la personalidad que se vinculan a la vida privada de las personas físicas. El derecho a la intimidad está en estrecha conexión con el derecho a la protección de datos personales ya que, ambos tienen como objeto garantizar que el individuo puede desarrollarse libremente, de forma que la protección de datos de carácter personal se encuentra vinculada con la garantía constitucional a la tutela de los derechos al honor, a la intimidad personal y a la propia imagen (art 18.1 y 18.4 CE).

En su inicio el desarrollo de estos derechos fundamentales se plasmó en primer lugar en la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (LORTAD) que fue derogada por la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (LOPD). Esta ley nació como un proyecto para reformar la LORTAD y finalmente terminó derogándola, con la finalidad de traspasar al ordenamiento interno los cambios introducidos, en materia de protección de datos, por la Directiva 95/46/CE sobre protección de datos personales, y garantizar y proteger las libertades públicas y los derechos fundamentales de las personas físicas.

De forma que en la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (LOPD), así como en el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprobó el Reglamento de desarrollo de la Ley Orgánica 15/1999 (RDPDP), se desarrollaron los derechos fundamentales consagrados en la Constitución, hasta que fueron desarrollados en la vigente Ley 3/2018 de 5 de diciembre, de protección de datos personales

y garantía de los derechos digitales (LOPDP). Esta ley no derogó expresamente el mencionado Real Decreto 1720/2007, de 21 de diciembre, de forma que seguirá siendo aplicable en todo lo que no se oponga a la ley, no obstante, deberá dictarse un reglamento nuevo ajustado a legalidad vigente.

Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (LORTAD) fue derogada por la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (LOPD).

PÉREZ GUTIÉRREZ[1] sostiene que la diferencia entre ambas leyes es que el ámbito de la LORTAD abarca los ficheros que contuviesen datos de carácter personal que se almacenasen en soporte electrónico, mientras que la LOPD amplía este ámbito a cualquier soporte, es decir, los ficheros en formato papel también están sujetos a esta reglamentación.

En el ámbito europeo encontramos otros antecedentes normativos sobre la protección de los datos personales consagrado como un derecho fundamental en la Carta de los Derechos Fundamentales de la Unión Europea y en el Tratado de Funcionamiento de la Unión Europea. En la Carta se recogen todos los derechos individuales, civiles, políticos, económicos y sociales que disfrutan todas las personas en la Unión Europea y, concretamente el artículo 8 establece que “toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan” y se dispone lo mismo en el artículo 16, párrafo 1 del Tratado de Funcionamiento de la Unión Europea. Cualquier persona que resida en la Unión, cuyos datos personales sean tratados en la Unión, o cuando dicho tratamiento se refiera a la oferta de bienes o servicios a dicha persona en la Unión o al control de su conducta en la Unión, está protegida por el marco jurídico adoptado por la Unión de conformidad con el artículo 8 de la Carta y con el artículo 16 del Tratado de Funcionamiento de la Unión Europea.

En el marco normativo comunitario la evolución de esta materia se plasma en:

- El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos. Este Reglamento derogó la Directiva 95/46/CE del Parlamento Europeo y del Consejo,

[1] PÉREZ GUITIÉRREZ, J. “LOPD: ¿Por qué? ¿Para quién?”, *Técnica económica: Administración y dirección de empresas,* n.175, 2006, pp. 53-56

de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respeta al tratamiento de datos personales y a la libre circulación de estos datos.

Este Reglamento se aplicó desde el 25 de mayo de 2018 y como establece su artículo 99 requirió la elaboración de una nueva ley orgánica que sustituyera a la Ley Orgánica 15/1999, de 13 de diciembre (LOPD).

- 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 a la libre circulación de dichos datos.

2.2 RÉGIMEN JURÍDICO VIGENTE

2.2.1 Normativa vigente sobre datos personales

Con estas premisas comunitarias entra en vigor la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales (LOPDP) que establece en su artículo 1 el doble objeto que persigue la norma:

1. Adaptar el ordenamiento jurídico español al Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos, y completar sus disposiciones. El derecho fundamental de las personas físicas a la protección de datos personales, amparado por el artículo 18.4 de la Constitución, se ejercerá con arreglo a lo establecido en el Reglamento (UE) 2016/679 y en esta ley orgánica.

2. Garantizar los derechos digitales de la ciudadanía conforme al mandato establecido en el artículo 18.4 de la Constitución.

El marco legal de referencia que desarrolla el derecho fundamental a la protección de datos personales lo establecen:

- El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 (Reglamento general de protección de datos, RGPD), y la
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPD).
  Con la entrada en vigor de esta ley queda derogada la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, sin perjuicio de lo previsto en la disposición adicional decimocuarta de la LOPD, y siguen vigentes las disposiciones de su Reglamento, aprobado por Real Decreto 1720/2007, de 21 de diciembre, que no contradigan, se opongan, o resulten incompatibles con lo dispuesto en el RGPD y la LOPD.

Respecto al tratamiento de datos personales relativos a condenas e infracciones penales, se aprueba la:

- Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales constituye la norma de referencia por la que se rige el tratamiento de este tipo de datos.
  Dicha Ley Orgánica traspone a nuestro ordenamiento jurídico la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 relativa a esta misma materia.

En materia de seguridad del tratamiento, resulta de aplicación, en virtud de la disposición adicional primera de la LOPD:

- El Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad y, en el ámbito ministerial,
- La Orden HFP/873/2021, de 29 de julio, que aprueba la Política de Seguridad de la Información en el ámbito de la Administración digital del Ministerio de Hacienda y Función Pública.

De manera que el marco legal normativo estatal queda configurado como se establece en la siguiente tabla:

• Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que

se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos, RGPD).
• Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, LOPD.
• Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.
• Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Vigente en los artículos referidos en la Disposición adicional decimocuarta y Disposición transitoria cuarta de la Ley Orgánica 3/2018, de 5 de diciembre.
• Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.
• Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
• Orden HFP/873/2021, de 29 de julio, por la que se aprueba la Política de Seguridad de la Información en el ámbito de la Administración digital del Ministerio de Hacienda y Función Pública.

2.2.2 Objeto de la legislación vigente

El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 (Reglamento General de Protección de Datos, RGPD) constituye la normativa básica para toda la UE, y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales es la norma que desarrolla en nuestro país ese reglamento.

En el artículo 1 del RGDP se determina el objeto del mismo:

- Protección de las personas físicas en lo que respecta al tratamiento de los datos personales y la libre circulación de tales datos.

- Protege los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales.
- Libre circulación de los datos personales en la Unión.
  Esta libre circulación no podrá ser restringida ni prohibida por motivos relacionados con la protección de las personas físicas en lo que respecta al tratamiento de datos personales.

Así mismo, en el artículo 1 de la LOPD se determina que el objeto de esta ley es:

- Adaptar el ordenamiento jurídico español al Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016 en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos.
- Ejercer con arreglo al Reglamento el derecho fundamental de las personas físicas a la protección de datos personales, amparado por el artículo 18.4 de la Constitución española.
- Garantizar los derechos digitales de la ciudadanía conforme al mandato del artículo 18.4 de la Constitución.

Y en su artículo 2, apartado 1 se establece que esta ley se aplicará a “cualquier 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”.

La Ley nace con la finalidad de garantizar la protección de la intimidad de las personas frente a los abusos que se puedan producir en el tratamiento de los datos personales que figuren o vayan a figurar en algún fichero.

El objeto de la ley es la tutela de la privacidad de las personas físicas entendida en el ámbito de su vida privada de forma que es la persona la que debe tener el control de los usos y finalidades a los que se destina la información relativa a su persona y evitar que sea usada para propósitos que previamente haya rechazado.

3. ÁMBITO DE APLICACIÓN MATERIAL Y TERRITORIAL DEL REGLAMENTO UE 2016/679 Y DE LA LEY ORGÁNICA 3/2018

3.1 INTRODUCCIÓN

La normativa sobre protección de datos, tanto el Reglamento General de Protección de Datos (RGPD) de 2016 como la Ley Orgánica 3/2018 de Protección de datos personales y garantía de los derechos digitales (LOPD), define un ámbito material de aplicación que abarca "cualquier tratamiento total o parcialmente automatizado de datos personales, así como el tratamiento no automatizado de datos personales destinados a ser incluidos en un fichero".

Esta amplia definición de "tratamiento de datos" abarca una amplia gama de operaciones realizadas sobre datos personales o conjunto de ellos, tanto automatizadas como manuales, como pueden ser la recogida, el registro, la organización, el almacenamiento, la conservación, la adaptación, la modificación, la extracción, la consulta, la utilización, la comunicación, la difusión, la habilitación de acceso, el cotejo, la interconexión, la limitación, la supresión o la destrucción. Es decir, engloba desde la recogida de datos personales hasta su destrucción.

No obstante, estas normativas establecen ciertas exclusiones específicas del ámbito de aplicación. Por ejemplo, se excluye el tratamiento de datos personales en actividades no comprendidas en el ámbito de aplicación del Derecho de la Unión Europea (UE), así como aquellos realizados por personas físicas para actividades personales o domésticas. También se excluyen los tratamientos realizados por autoridades competentes en el contexto de la prevención, investigación o enjuiciamiento de infracciones penales.

Además, la aplicación del RGPD ha suscitado interpretaciones divergentes en cuanto a su ámbito material, especialmente en lo que respecta a la definición de tratamiento de datos personales. Mientras que el RGPD parece establecer que cualquier tratamiento automatizado o parcialmente automatizado de datos personales está sujeto a la regulación, existen interpretaciones que sugieren que solo se considera tratamiento aquel que implica operaciones activas sobre los datos, excluyendo aquellos datos que simplemente se almacenan en un fichero sin ser procesados activamente.

Esta discrepancia de interpretación plantea incertidumbres sobre la aplicación práctica de la normativa y la protección efectiva de los datos personales. Se espera que las autoridades de protección de datos y los tribunales aclaren estas cuestiones para garantizar una interpretación coherente y proporcionar seguridad jurídica en este ámbito.

Según el estudio de Berrocal Lanzarot, A. I. (2019) [2] se afirma que esta normativa afecta a diversas áreas de la sociedad y la economía, así como su impacto en la privacidad de los individuos y la regulación de las actividades comerciales en el entorno digital.

En la era de la economía digital, los datos personales se han convertido en un activo invaluable para las empresas y organizaciones. La recopilación, almacenamiento y procesamiento de estos datos alimenta el motor de la publicidad en línea, la personalización de servicios y la toma de decisiones empresariales. Sin embargo, la reciente normativa sobre protección de datos ha impuesto restricciones significativas en la forma en que las empresas pueden utilizar los datos personales de los individuos. Las multas por incumplimiento pueden ser sustanciales, lo que obliga a las empresas a adoptar medidas más rigurosas para garantizar el cumplimiento de la ley.

Además, la protección de la privacidad y los derechos individuales es otro pilar fundamental de la normativa sobre protección de datos. Esta legislación busca garantizar que los individuos tengan control sobre sus datos personales y que su información no sea utilizada de manera indebida o sin su consentimiento. En un mundo donde la recopilación masiva de datos es omnipresente, estas regulaciones son esenciales para proteger la autonomía y la dignidad de las personas.

Por último, la normativa sobre protección de datos también tiene un impacto significativo en la regulación de las prácticas comerciales en línea. Las empresas están obligadas a obtener el consentimiento explícito de los usuarios antes de recopilar y procesar sus datos personales. Además, deben proporcionar información clara y transparente sobre cómo se utilizarán estos datos. Esto ha llevado a un cambio en la forma en que las empresas recopilan y gestionan la información de los clientes, promoviendo una mayor transparencia y responsabilidad en el tratamiento de datos.

La Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales (LOPD) y el Reglamento General de Protección de Datos (RGPD) de 2016 establecen un marco normativo para la protección de datos personales que aborda aspectos cruciales en la era digital. Uno de los aspectos fundamentales es el ámbito material de aplicación de estas normativas, que define el alcance de su protección sobre los datos personales.

[2]BERROCAL LANZAROT, A. I.: *Estudio jurídico-crítico sobre la ley orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales*, Editorial Reus, Madrid, 2019.

3.2 ÁMBITO DE APLICACIÓN MATERIAL DEL REGLAMENTO UE 2016/679 Y DE LA LEY ORGÁNICA 3/2018

El ámbito de aplicación material del Reglamento UE 2016/679, RGPD está regulado en su artículo 2, como ocurre con el ámbito de aplicación de la Ley Orgánica 3/2018, LOPD, con el que comparte, al menos en su primer apartado, la misma redacción.

De forma que el RGPD en su artículo 2, apartado 1 establece que este reglamento 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. Y la LOPD comparte la misma redacción respecto del ámbito de aplicación en su artículo 2, apartado 1.

La Ley Orgánica 3/2018 establece en sus Títulos I a IX y en los artículos 89 a 94 una serie de derechos y regulaciones específicas relacionadas con la protección de datos personales y los derechos digitales en diversos contextos, como el lugar de trabajo y el uso de tecnologías digitales.

Estas disposiciones se aplican a cualquier tratamiento de datos personales, ya sea total o parcialmente automatizado, así como al tratamiento no automatizado de datos personales que estén contenidos o destinados a ser incluidos en un fichero.

Sin embargo, hay ciertos casos en los que la ley orgánica no será aplicable. Además, para los tratamientos de datos que no estén directamente sujetos al Reglamento de la Unión Europea debido a que afectan a actividades fuera del ámbito de aplicación del Derecho de la Unión Europea, se aplicará la legislación específica correspondiente, si la hubiere, y supletoriamente lo dispuesto en el Reglamento y en la Ley Orgánica. Esto incluye tratamientos como los realizados en el marco de la legislación orgánica del régimen electoral general, en instituciones penitenciarias, así como aquellos derivados del Registro Civil y otros registros públicos.

Por otro lado, el tratamiento de datos llevado a cabo en el contexto de procesos judiciales y dentro de la gestión de la Oficina Judicial se regirá por lo dispuesto en el Reglamento de la Unión Europea y la Ley Orgánica, sin perjuicio de las disposiciones de la Ley Orgánica 6/1985, del Poder Judicial, que sean aplicables.

Esta regulación garantiza una protección adecuada de los datos personales y los derechos digitales en diversos ámbitos, asegurando su adecuada gestión y respeto en conformidad con las leyes y regulaciones pertinentes.

3.3 ÁMBITOS EN LOS QUE NO SE APLICA EL REGLAMENTO UE 2016/679 Y LA LEY ORGÁNICA 3/2018

La LOPD establece el artículo 2, apartado 2 los casos en los que esta ley no será aplicable:

a) A los tratamientos de datos excluidos del ámbito de aplicación del Reglamento general de protección de datos de la Unión Europea, según lo establecido en su artículo 2.2.
b) A los tratamientos de datos de personas fallecidas, sin perjuicio de lo establecido en el artículo 3 de esta misma ley.
c) A los tratamientos de datos sometidos a normativas específicas sobre protección de materias clasificadas.

El artículo 2, apartado 2 del RGPD establece los supuestos en que no se aplica el Reglamento al tratamiento de datos personales:

a) En el ejercicio de una actividad no comprendida en el ámbito de aplicación del Derecho de la Unión.
b) Por parte de los Estados miembros cuando lleven a cabo actividades 3comprendidas en el ámbito de aplicación del capítulo 2 del título V del TUE.
c) Efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas.
d) por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención.

3.4 ÁMBITO TERRITORIAL

El artículo 3 del RGPD establece el ámbito territorial donde se aplica el Reglamento:

1. Al tratamiento de datos personales 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.
2. Al tratamiento de datos personales de interesados que residan en la Unión por parte de un responsable o encargado no establecido en la Unión, cuando las actividades de tratamiento estén relacionadas con:
    a) la oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si a estos se les requiere su pago, o

b) el control de su comportamiento, en la medida en que este tenga lugar en la Unión.

3. Al tratamiento de datos personales por parte de un responsable que no esté establecido en la Unión sino en un lugar en que el Derecho de los Estados miembros sea de aplicación en virtud del Derecho internacional público.

4. DEFINICIÓN Y CLASIFICACIÓN DE LOS DATOS PERSONALES

4.1 DEFINICIÓN

El artículo 4 del RDGP define los “datos personales” como 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.

Los datos de carácter personal son toda información relativa a una persona física viva identificada o identificable. También son datos personales toda información que, recopilada y puesta en relación, pueda llevar a la identificación de una determinada persona.

Por lo tanto, los datos de carácter personal son toda aquella información relativa a personas físicas vivas que pueda usarse para identificarlas, tanto si se trata de información personal sobre su identidad como si es respecto a sus ocupaciones, hábitos o situación personal.

Los identificadores son piezas de información a partir de las cuales se puede identificar a una persona, ya que mantienen una relación privilegiada y cercana con el interesado. Por lo tanto, en ese sentido, se consideran datos de una persona.

Según la LOPD, los datos personales son cualquier información sobre una persona viva, donde esa persona está identificada o podría ser identificada. Pueden cubrir varios tipos de información, como el nombre, la fecha de nacimiento, la dirección de correo electrónico, el número de teléfono, la dirección, las características físicas o los datos de ubicación, una vez que esté claro con quién se relaciona esa información, o si es razonablemente posible averiguarlo.

Los datos personales no tienen que estar en forma escrita, también pueden ser información sobre cómo se ve o suena un sujeto de datos, por ejemplo, fotos o grabaciones de audio o video.

Con carácter general diferenciamos tres tipos de datos personales:

- Datos básicos de una persona (nombre y apellidos, dirección postal, número de teléfono, DNI, etc.).
- Datos sensibles (que son aquellos datos cuyo tratamiento puede suponer un riesgo para los derechos y libertades fundamentales de los interesados).
- Los ya citados indicadores que pueden identificar o hacer identificable a una persona (dirección IP, la huella digital, etc.).

4.2 CLASIFICACIÓN DE DATOS PERSONALES SEGÚN EL RGPD

El RGPD clasifica los datos personales en tres categorías de datos personales diferentes, en función del riesgo que su tratamiento supone para los derechos y libertades de los interesados y las obligaciones que se deben cumplir para poder tratarlos.

4.2.1 Datos de carácter general

Cualquier dato de carácter personal que no esté contemplado en las categorías de datos especiales, es considerado un dato personal general u ordinario.

Los datos personales ordinarios pueden incluir detalles de identificación personal como nombre y dirección, relaciones con los clientes, finanzas personales, asuntos relacionados con impuestos, deudas, días de enfermedad, circunstancias relacionadas con el trabajo, circunstancias familiares, residencia, automóvil, calificaciones, solicitudes, CV, fecha de empleo, puesto, área de trabajo, teléfono del trabajo, datos clave: nombre, dirección, fecha de nacimiento, dirección IP u otra información similar no sensible.

4.2.2 Datos de carácter personal especialmente protegidos

Los datos de categorías especiales son los datos de carácter personal especialmente protegidos, puesto que revelan información que puede tener impacto sobre los derechos y libertades fundamentales de las personas, pudiendo exponerlas a la discriminación y por ello deben tratarse con mayor cuidado y aplicarse mayores medidas de seguridad.

Estas categorías de datos especiales son:

- Origen étnico o cultural: Este tipo de datos se refieren a la raza o etnia de las personas. La etnia es la creencia subjetiva en una procedencia común. Esa creencia puede

basarse en semejanzas de aspecto exterior, costumbres, idioma, religión o memoria de eventos históricos como migraciones.

- Opiniones políticas, religiosas y filosóficas: Esto incluye todos aquellos datos referidos a la religión o creencia de una persona y sus opiniones políticas.
- Orientación sexual: Son los datos sobre la orientación sexual y el género. Estos son aspectos importantes de nuestra identidad.
- Afiliación sindical: Los datos sobre afiliación sindical son los que indican si una persona concreta está afiliada a un sindicato.
- Datos genéticos: Son datos personales relacionados con las características genéticas heredadas o adquiridas de una persona física que proporcionan información única sobre la fisiología o la salud de esa persona física y que resultan, en particular, de un análisis de una muestra biológica de la persona física en cuestión. Esto incluye análisis cromosómico, de ADN o ARN, o cualquier otro tipo de análisis que le permita obtener información equivalente. Cuando la información genética se haya anonimizado, ya no se considerará dato personal.
- Datos biométricos: Los datos biométricos son datos personales resultantes de un procesamiento técnico específico relacionado con las características físicas, fisiológicas o de comportamiento de una persona física, que permiten o confirman la identificación única de esa persona física, como imágenes faciales o datos dactiloscópicos (huellas dactilares) o análisis de firmas manuscritas. Se consideran datos de categorías especiales cuando su finalidad es identificar de manera única a una persona física (como, por ejemplo, en los controles de acceso).
- Datos relativos a la salud: Son datos personales relacionados con la salud física o mental de una persona física, incluida la prestación de servicios de atención médica, que revelan información sobre su estado de salud. Los datos de salud pueden referirse al estado de salud pasado, actual o futuro de una persona. No solo cubre detalles específicos de condiciones médicas, pruebas o tratamientos, sino que incluye cualquier dato relacionado que revele algo sobre el estado de salud de una persona. Por tanto, los datos sanitarios pueden incluir una amplia gama de datos personales, por ejemplo:
  - Cualquier información sobre lesiones, enfermedades, discapacidades o riesgos de enfermedades, incluidos antecedentes médicos, opiniones médicas, diagnóstico y tratamiento clínico.
  - Datos de exámenes médicos, resultados de pruebas, datos de dispositivos médicos o datos de rastreadores de actividad física.

- Información recopilada del individuo cuando se registra para los servicios de salud o accede al tratamiento.
- Detalles de citas, recordatorios y facturas que informan sobre la salud de la persona. Estos se incluyen en «la prestación de servicios de atención médica», pero deben revelar algo sobre el estado de salud de una persona. Por ejemplo, una cita con el médico de cabecera o el hospital de forma aislada no le dirá nada sobre la salud de una persona, ya que puede ser una cita de control o evaluación. Sin embargo, podría inferir razonablemente datos de salud de la lista de citas de una persona en una clínica de osteópata o de una factura por una serie de sesiones de fisioterapia.

4.2.3 Datos personales de naturaleza penal

Los datos personales sobre denuncias, procedimientos o condenas penales no son datos de categoría especial. Sin embargo, existen reglas y salvaguardas similares para procesar este tipo de datos, para hacer frente a los riesgos particulares asociados a ellos.

Para procesar datos personales sobre condenas o delitos penales, debe existir una base legal y una autoridad legal o autoridad oficial para el procesamiento. También se puede procesar este tipo de datos si se tiene autoridad oficial para hacerlo porque se está procesando los datos a título oficial.

No se puede llevar un registro completo de condenas penales a menos que se haga a título oficial.

4.3 EJEMPLOS DE DATOS PERSONALES Y DE QUÉ NO SON DATOS DE CARÁCTER PERSONAL

Según la normativa son ejemplos de datos personales:

1- Datos personales de carácter general
• Nombre y apellido • Dirección de correo electrónico • Dirección de la casa (calle, código postal, código postal, ciudad) • Número de teléfono • Foto • Fecha de nacimiento

- Lugar / ciudad / país de nacimiento
- Número de cuenta bancaria
- Número de tarjeta de crédito
- Número de seguridad social
- Número de pasaporte, número de identificación nacional, número de licencia de conducir
- Número de placa de matrícula del vehículo
- Número de empleado
- Dirección IP
- ID de cookie
- Datos de localización
- La escritura (la forma en la que escribimos)
- Contraseña
- ID / enlaces de perfil de redes sociales
- ID de dispositivo móvil
- Historial de empleo, título del trabajo
- Historia académica

2- Datos de carácter personal especialmente protegidos

- Nacionalidad
- Sexo / género
- La etnia o la raza
- La historia clínica
- La afiliación sindical
- La ideología política

No son datos de carácter personal:

- Aquella información que no lleve a identificar a una persona; en concreto, no se consideran datos de carácter personal los datos anonimizados, siempre y cuando no sea posible reidentificar a la persona física a la que se refieren.
- Tampoco se considera un dato personal los datos de personas jurídicas, incluido el nombre y la forma de persona jurídica y sus datos de contacto.

5. EL INDIVIDUO COMO SUJETO DE LA PROTECCIÓN LEGAL: LOS DATOS PERSONALES DE LAS PERSONAS FALLECIDAS

5.1 INTRODUCCIÓN

Los datos personales representan cualquier información relativa a una persona física viva identificada o identificable y, determinadas menciones como el nombre y los apellidos, el número de identificación fiscal, los datos de geolocalización, la dirección de protocolo de internet (IP), datos clínicos en poder de un médico, etc. son distintas informaciones, que debidamente recopiladas pueden identificar a una persona y por ello son datos de carácter personal que sólo se protegen si la persona titular de los mismos se encuentra efectivamente viva.

Así lo afirma la Comisión Europea, y queda reflejado en el Considerando 27 del Reglamento (UE) 2016/679/UE, de 27 de abril de Protección de Datos, donde se determina que dicho Reglamento no se aplica a la protección de datos personales de personas fallecidas, sin perjuicio de la habilitación que se efectúa en favor de los Estados miembros de la Unión Europea, ya que estos son competentes para establecer normativa *ad hoc* en sus ordenamientos jurídicos internos, que regulen el régimen jurídico de los datos personales de las personas fallecidas. Así se hizo en el artículo 2. 2º de nuestra Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, donde se ratifica lo dispuesto en el RGPD, en el sentido de que esta ley orgánica no será aplicable a los tratamientos de datos de personas fallecidas.

5.2 DATOS PERSONALES DE LAS PERSONAS FALLECIDAS, MENORES Y PERSONAS CON DISCAPACIDAD FALLECIDAS

La Ley Orgánica 3/2018 establece disposiciones específicas relacionadas con el acceso a los datos personales de personas fallecidas y la protección de sus derechos digitales. Estas disposiciones garantizan un marco legal claro para el manejo de los datos personales de personas fallecidas, asegurando el respeto a su voluntad y la protección de sus derechos incluso después de su fallecimiento.

En su artículo 3 establece que las personas vinculadas al fallecido por razones familiares o, de hecho, así como sus herederos, tienen derecho a dirigirse al responsable o encargado del tratamiento de datos para solicitar el acceso, rectificación o supresión de los datos personales del fallecido. Sin embargo, existen excepciones a este derecho en casos en

los que la persona fallecida lo haya prohibido expresamente o cuando lo establezca la ley. Esta prohibición no afecta al derecho de los herederos de acceder a los datos de carácter patrimonial del fallecido.

Además, las personas o instituciones designadas expresamente por el fallecido también pueden solicitar el acceso a sus datos personales, así como su rectificación o supresión, de acuerdo con las instrucciones recibidas. Surge la necesidad de un real decreto para establecer los requisitos y condiciones para acreditar la validez y vigencia de estos mandatos e instrucciones, así como un posible registro de los mismos.

En caso de fallecimiento de menores, estas facultades pueden ser ejercidas por sus representantes legales o, en el marco de sus competencias, por el Ministerio Fiscal, que puede actuar de oficio o a instancia de cualquier persona física o jurídica interesada.

Por último, en el caso de fallecimiento de personas con discapacidad, estas facultades pueden ser ejercidas por quienes hayan sido designados para el ejercicio de funciones de apoyo, siempre que estas facultades estén comprendidas en las medidas de apoyo prestadas por el designado.

Estas disposiciones con relación a los datos personales post mortem, se complementa con el reconocimiento en el artículo 96 de la LOPDGDD del llamado “testamento digital”, que abre nuevos cauces con relación a la voluntad de los causantes sobre dichos datos, para un momento posterior a la muerte.

La problemática relativa al testamento digital está alcanzando mucho interés, ya que es necesario regular y dar seguridad jurídica a múltiples informaciones y contenidos sobre las personas que fallecen, y que se pueden encontrar en numerosos dispositivos de carácter tecnológico, y aplicaciones, tales como: el rastro digital de la persona fallecida; las cuentas de usuario registradas; las suscripciones a aplicaciones o servicios webs de todo tipo; las inscripciones y el contenido que el difunto haya incorporado a las diversas redes sociales, las cuentas de correo electrónico, los blogs o las webs de que sea titular, las contraseñas de los dispositivos, los dominios, el dinero virtual, toda la información que el fallecido tenga en la nube (Dropbox, One Drive, Google Drive, o cualquier otro sistema de almacenamiento en la nube, etc.), su disco duro del ordenador, la huella digital del mismo, los bitcoins o cualquier otra clase de criptomoneda que tenga en sus wallets, las claves del ordenador y de los programas, la información que sobre el mismo esté en la red en cualquier forma, entre otros múltiples aspectos.

Es evidente que la normativa que debe prever el destino de estos datos y contenidos post mortem son elementos difíciles de compatibilizar, no siendo suficiente a estos efectos la existencia de una norma que atienda exclusivamente a la problemática surgida sobre la base de la protección de datos personales, ya que confluyen múltiples vertientes o aspectos del derecho como las cuestiones atinentes a los derechos hereditarios, que también deben ser protegidas. En este sentido, se deben tener presente las facultades que ahora se reconocen a los albaceas testamentarios o a aquella persona o institución a la que el fallecido hubiese designado expresamente para ello. También podrán solicitar, con arreglo a las instrucciones recibidas, el acceso a los contenidos con vistas a dar cumplimiento a las instrucciones recibidas del causante, y poder disponer de los mismos, lo que a veces dificultará el hecho de hacer compatible la existencia de dichos derechos, con los legítimos derechos de los herederos.

A título de ejemplo se puede citar el hecho de que un causante tenga grabaciones en Youtube, sobre las que el albacea haya recibido instrucciones de borrado, cuando representen un valor económico, afectivo o sentimental, que los herederos tengan que preservar. Consecuentemente con todo lo anterior, nos encontramos con una nueva perspectiva del derecho, que en un futuro no muy cercano generará múltiples conflictos, y donde las exigencias y prácticas sociales unidas al desarrollo tecnológico, cada día van a ir reclamando una mayor regulación que compatibilice todos los intereses en disputa.

5.3 EL CONSENTIMIENTO

El Reglamento General de Protección de Datos (RGPD) de la Unión Europea establece directrices claras sobre el consentimiento en el contexto del tratamiento de datos personales

En su artículo 4, establece que el «consentimiento del interesado» es toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen.

Este consentimiento debe ser obtenido mediante un acto afirmativo claro que demuestre una clara elección por parte del individuo, y no puede ser inferido por la inacción o la falta de respuesta del interesado. Además, debe ser fácilmente revocable en cualquier momento.

El RGPD exige que el consentimiento sea verificable, es decir, que el responsable del tratamiento pueda demostrar que se obtuvo el consentimiento del interesado de acuerdo con las normativas establecidas. Esto implica que la obtención y gestión del consentimiento deben ser documentadas y transparentes, asegurando que el individuo tenga control sobre sus datos personales en todo momento.

Asimismo, la Ley Orgánica 3/2018, de 5 de diciembre (LOPD) en su artículo 6 muestra su conformidad con la definición que hace el RGPD sobre el consentimiento del afectado y el tratamiento de los datos personales basado en el consentimiento del interesado.

Esto implica que el consentimiento debe ser:

1. Libre: el interesado debe tener la capacidad de decidir sin presiones indebidas.
2. Específico: debe referirse de manera clara y precisa a cada uno de los tratamientos concretos que se pretenden llevar a cabo con los datos.
3. Informado: el interesado debe tener conocimiento de la existencia del tratamiento, de la finalidad del mismo, de los derechos que le asisten y de cómo ejercerlos.
4. Inequívoco: debe ser claro y no dejar lugar a dudas sobre la aceptación del tratamiento de los datos.

Es esencial que el consentimiento se obtenga antes de iniciar cualquier tratamiento de datos personales, y que sea revocable en cualquier momento sin formalidades excesivas.

En resumen, el consentimiento bajo el prisma del RGPD y de la LOPD requiere transparencia, claridad y acción afirmativa por parte del individuo, garantizando así la protección de sus derechos fundamentales en relación con el tratamiento de sus datos personales.

5.4 EL INDIVIDUO COMO EJE CENTRAL EN LA GESTIÓN DE CONTROL DE DATOS

Hoy en día, nos enfrentamos a nuevos retos en relación con nuestra privacidad y la seguridad de nuestros datos personales. La mayor parte de los usuarios de internet están preocupados de que su información personal pueda ser robada o utilizada de algún modo sin su permiso. Es urgente poder garantizar a las personas el conocimiento y control de sus datos personales en todo momento.

El artículo 4, apartado 11 del Reglamento (UE) 2016/679, define el "consentimiento del afectado" como toda manifestación de voluntad libre, específica, informada e inequívoca por la que este acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen.

Cuando se pretenda fundar el tratamiento de los datos en el consentimiento del afectado para una pluralidad de finalidades será preciso que conste de manera específica e inequívoca que dicho consentimiento se otorga para todas ellas.

Respecto a los menores de edad el tratamiento de sus datos personales únicamente podrá fundarse en su consentimiento cuando sea mayor de catorce años. Se exceptúan los supuestos en que la ley exija la asistencia de los titulares de la patria potestad o tutela para la celebración del acto o negocio jurídico en cuyo contexto se recaba el consentimiento para el tratamiento.

Asimismo, el tratamiento de los datos de los menores de catorce años, fundado en el consentimiento, solo será lícito si consta el del titular de la patria potestad o tutela, con el alcance que determinen los titulares de la patria potestad o tutela.

En el momento actual, las grandes plataformas son las que cuentan con los recursos necesarios para recopilar, comerciar y tomar decisiones basadas en nuestros datos personales – mientras que los individuos solo pueden aspirar a obtener cierto control sobre lo que ocurre con sus datos, realizando previamente un gran esfuerzo para ello.

Por ese motivo surgen iniciativas de organizaciones sin ánimo de lucro, como MyData Global, que promueven la gestión de datos personales centrada en el individuo y abogan por garantizar el derecho de las personas a participar activamente en la *economía del dato,* con la finalidad de construir una sociedad digital más justa, segura, sostenible y próspera, cuyos pilares sean:

- Establecer relaciones de confianza y seguridad entre las personas y las organizaciones.
- Conseguir la autonomía en materia de datos, no sólo mediante la protección legal, sino también con medidas para compartir y distribuir el poder de los datos.
- Maximizar los beneficios colectivos de los datos personales, compartiéndolos equitativamente entre las organizaciones, los individuos y la sociedad.

La comunidad de MyData ha estado trabajando durante años para promover una visión más centrada en las personas en lo que respecta a la gestión, tratamiento y uso de los datos. A través de su participación en proyectos como el Data Spaces Support Centre, buscan establecer el futuro del uso y gobierno responsable de los datos en la Unión Europea.

Los principios de MyData son:

1. Control de los datos centrado en las personas

Las personas deben tener el poder de decidir sobre la gestión de todos los aspectos de su vida personal. Esto implica disponer de herramientas prácticas que les permitan entender y controlar quién accede a sus datos y cómo se utilizan y comparten. La privacidad, la seguridad y el uso mínimo de datos deben ser prácticas estándar en el diseño de aplicaciones, y las condiciones de uso de los datos personales deben ser negociadas de manera justa entre individuos y organizaciones.

2. Las personas como punto central de integración

El valor de los datos personales aumenta con su diversidad, lo cual también incrementa las amenazas a la privacidad. Esta contradicción aparente puede resolverse colocando a las personas en el centro de cualquier intercambio de datos, siempre priorizando sus necesidades sobre cualquier otra motivación.

3. Autonomía individual

En una sociedad impulsada por los datos, los individuos deben ser vistos como agentes libres y autónomos, capaces de establecer y perseguir sus propios objetivos.

4. Portabilidad, acceso y reutilización

Permitir que las personas puedan obtener y reutilizar sus datos personales para sus propios fines y en diferentes servicios es clave para superar los silos de datos aislados, transformando los datos en recursos reutilizables. La portabilidad de datos no debe ser solo un derecho legal, sino que debe combinarse con medios prácticos que faciliten la transferencia segura y sencilla de los datos a otros servicios o dispositivos personales.

5. Transparencia y responsabilidad

Las organizaciones que utilizan los datos personales deben ser transparentes respecto al uso que hacen de ellos y la finalidad de dicho uso. Al mismo tiempo, deben asumir su responsabilidad sobre la gestión que hacen de esos datos, incluido cualquier incidente de seguridad.

6. Interoperabilidad

Es necesario minimizar la fricción en el flujo de datos desde las fuentes de origen a los servicios que los utilizan. Para ello hay que incorporar los efectos positivos de los ecosistemas abiertos e interoperables, incluyendo protocolos, aplicaciones e infraestructura. Esto se logrará a través de la aplicación de normas y prácticas comunes y estándares técnicos.

Y este año en la nueva edición de MyData Conference mostrará casos prácticos en los que la recopilación, el procesamiento y el análisis el análisis de los datos personales sirven principalmente a las necesidades y experiencias de los seres humanos.

6. RESPONSABLE DEL TRATAMIENTO DE DATOS, ENCARGADO DEL TRATAMIENTO Y DELEGADO DE PROTECCIÓN DE DATOS

6.1 RESPONSABLE DEL TRATAMIENTO

La normativa sobre protección de datos contempla la figura del responsable y el encargado del tratamiento de datos. Estos actores tienen responsabilidades específicas en cuanto a la gestión y protección de la información personal, estableciendo pautas claras sobre sus roles y obligaciones.

El RGPD define en su artículo 4 al "**responsable del tratamiento**" o "**responsable de datos**" como 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.

Se encarga de determinar los fines y medios para el tratamiento, así como de establecer las medidas técnicas y organizativas que garanticen la seguridad de los datos. Debe informar sobre la finalidad del tratamiento y los medios elegidos para ello, así como informar si los datos van a ser tratados por terceros. Como su nombre indica, tiene la responsabilidad de garantizar la confidencialidad, integridad y disponibilidad de los datos personales que le han sido comunicados o cedidos. Además, debe ser capaz de demostrar el cumplimiento del RGPD y la LOPDGDD ante las autoridades de control.

El responsable del tratamiento es quien decide si quiere contar con la ayuda de un encargado del tratamiento, o si decide realizar el tratamiento de datos por sí mismo.

El artículo 24 del RGPD señala de forma general los objetivos del responsable del tratamiento de datos personales, haciendo hincapié en su obligación de aplicar las medidas técnicas y organizativas necesarias para garantizar el cumplimiento de la ley conforme a lo dispuesto en el propio Reglamento.

Las principales obligaciones del responsable del tratamiento de datos son:

- Llevar un registro de las actividades de tratamiento.

  Estos registros de actividades de tratamiento de datos personales son obligatorios para empresas con más de 250 empleados, cuando se tratan datos personales a gran escala de manera sistemática, o se traten datos de categorías especiales, lo que supone un riesgo para los derechos y libertades fundamentales de los individuos.

- Deber de información.

  El RGPD señala que se ha de informar a los usuarios sobre los datos que se recaban, con qué finalidad, durante cuánto tiempo, si se van a ceder a terceros, o las vías para ejercer sus derechos ARCO (Acceso, Rectificación, Supresión, Limitación del tratamiento, Portabilidad y Oposición).

  También se debe informar sobre si los datos se usarán para elaborar perfiles para la toma de decisiones automatizadas. La elaboración de perfiles es el tratamiento automatizado de datos de carácter personal con la finalidad de evaluar, estudiar, analizar o hacer predicciones sobre las personas.

- Consentimiento expreso.

  Para poder tratar los datos personales, el responsable ha de obtener el consentimiento expreso, inequívoco, explícito y voluntario de sus titulares.

- Análisis de riesgos y evaluaciones de impacto.

  Con carácter previo a cualquier tratamiento, se deben realizar análisis de riesgos con el objetivo de determinar los riesgos derivados del mismo y las medidas de seguridad a adoptar para mitigarlos.

  Cuando del análisis de riesgos se concluya que existe un nivel de riesgo elevado para los derechos y libertades de los individuos, el responsable del tratamiento habrá de realizar evaluaciones de impacto.

  Estas evaluaciones de impacto en protección de datos también son obligatorias cuando el tratamiento concierna a datos de categorías especiales (art.9 del RGPD).

- Medidas y procedimientos.
  El responsable será quien determine las medidas técnicas y organizativas necesarias para garantizar la seguridad e integración de los datos, y su protección frente a robos, pérdidas accidentales o accesos no autorizados.

- Nombramiento del Delegado de Protección de Datos.
  En caso de ser necesario, el responsable nombrará un Delegado de Protección de Datos. El *data protection officer* es una de las novedades del Reglamento. Es la persona encargada del cumplimiento de la normativa de protección de datos en las empresas y organizaciones que deban designarlo obligatoriamente o las que lo hagan de forma voluntaria
  El artículo 37 del RGPD y el artículo 34 de la LOPDGDD determinan qué entidades necesitan contar con esta figura.

- Notificación de brechas de seguridad.
  Los responsables del tratamiento han de notificar las brechas de seguridad a la autoridad de protección de datos competente. El plazo máximo para notificar estas brechas de seguridad es de 72 horas.

6.2 ENCARGADO DEL TRATAMIENTO DE DATOS

El RGPD define en su artículo 4 al "**encargado del tratamiento**" o "**encargado**" como la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento.

El encargado realiza el tratamiento siguiendo las directrices y empleando los medios designados por el responsable. Asimismo, debe asistir al responsable a petición de éste, para asegurar que se cumplen todas las obligaciones en materia de protección de datos.

El responsable debe elegir un encargado del tratamiento que ofrezca las garantías suficientes para implantar las medidas técnicas y organizativas necesarias para que el tratamiento se adapte a las exigencias del RGPD.

El encargado no podrá subcontratar los servicios de un subencargado del tratamiento, salvo autorización expresa del responsable.

Un ejemplo de responsable y el encargado del tratamiento de datos es una clínica de tratamientos y cirugía estética que trata datos personales de sus clientes, empleados o proveedores. La clínica estética actuará como responsable del tratamiento de los datos. Sin embargo, puede tener contratados los servicios de una asesoría que le gestione la contabilidad, los impuestos, los contratos, facturas, nóminas, etc. La asesoría será el encargado del tratamiento de datos.

6.3 REGULACIÓN DE LA RELACIÓN ENTRE EL RESPONSABLE Y EL ENCARGADO DEL TRATAMIENTO DE DATOS.

La regulación de la relación entre el **responsable** y el **encargado del tratamiento de datos** busca asegurar que los datos personales se manejen con el máximo nivel de protección y seguridad. Dicha relación entre ambos se regula a través de un contrato o acto jurídico vinculante con arreglo al derecho de la Unión Europea o de sus Estados miembros.

El contrato se realizará por escrito y en ese documento se estipularán claramente las condiciones y términos del tratamiento de datos personales. Entre los aspectos que debe contener se incluyen:

- Objeto, duración, naturaleza y finalidad del tratamiento.
- Tipo de datos personales y categorías de interesados.
- Obligaciones y derechos del responsable.
- Contenido Específico del Contrato

Y respecto a las obligaciones del encargado del tratamiento de datos hacia el responsable, el contrato debe incluir, como mínimo las siguientes:

- Tratar los datos personales solo siguiendo las instrucciones documentadas del responsable, incluyendo las transferencias internacionales de datos a un tercer país o a una organización internacional.
- Garantizar que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación legal de confidencialidad.
- Tomar todas las medidas de seguridad necesarias establecidas en el artículo 32 del RGPD, con el fin de garantizar la seguridad e integridad de los datos.

- No subcontratar el tratamiento de datos a otro encargado sin la autorización previa y por escrito del responsable.
- Ayudar al responsable a garantizar el cumplimiento de las obligaciones relativas a los derechos de los interesados.
- Asistir al responsable en el cumplimiento de sus obligaciones de seguridad, notificación de violaciones de seguridad de los datos, realización de evaluaciones de impacto y consultas previas con las autoridades de protección de datos.
- Suprimir o devolver todos los datos personales al finalizar la prestación de servicios de tratamiento.
- Poner a disposición del responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en el RGPD y permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte del responsable o de otro auditor autorizado por dicho responsable.

Aunque el encargado actúe bajo las instrucciones del responsable, ambos son responsables de cumplir con las obligaciones de protección de datos. En caso de incumplimiento, tanto el responsable como el encargado pueden estar sujetos a sanciones ya que tienen la responsabilidad compartida.

Ambas figuras deben colaborar en:

- Hacer efectivo el ejercicio de los derechos de los interesados respecto a los derechos de acceso, rectificación supresión, oposición y portabilidad de datos;
- Las transferencias internacionales de datos, ya que cuando se da el caso de que el encargado del tratamiento se encuentra en un país tercero, fuera de la Unión Europea debe asegurar mecanismos adecuados de protección de esos datos, como:
    - Cláusulas contractuales tipo adoptadas por la Comisión Europea
    - Normas corporativas vinculantes
    - O certificaciones y códigos de conducta aprobados.

En definitiva, la diferencia entre responsable y encargado de tratamiento de datos es más profunda de lo que podemos pensar. En realidad, son dos figuras totalmente distintas pero que pueden estar relacionadas. Ambas pueden ser los responsables de la gestión de los datos personales, con la diferencia de que el encargado siempre lo hará por cuenta del responsable.

6.4 DELEGADO DE PROTECCIÓN DE DATOS EN LA LOPD

La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales en su artículo 34 establece que los responsables y encargados del tratamiento deberán designar un **delegado de protección de datos** en los supuestos previstos en el artículo 37.1 del Reglamento (UE) 2016/679 y, en todo caso, cuando se trate de las siguientes entidades:

a) Los colegios profesionales y sus consejos generales.
b) Los centros docentes que ofrezcan enseñanzas en cualquiera de los niveles establecidos en la legislación reguladora del derecho a la educación, así como las Universidades públicas y privadas.
c) Las entidades que exploten redes y presten servicios de comunicaciones electrónicas, cuando traten habitual y sistemáticamente datos personales a gran escala.
d) Los prestadores de servicios de la sociedad de la información cuando elaboren a gran escala perfiles de los usuarios del servicio.
e) Las entidades incluidas en el artículo 1 de la Ley 10/2014, de 26 de junio, de ordenación, supervisión y solvencia de entidades de crédito.
f) Los establecimientos financieros de crédito.
g) Las entidades aseguradoras y reaseguradoras.
h) Las empresas de servicios de inversión
i) Los distribuidores y comercializadores de energía eléctrica y gas natural.
j) Las entidades responsables de ficheros comunes para la evaluación de la solvencia patrimonial y crédito o de los ficheros comunes para la gestión y prevención del fraude, incluyendo a los responsables de los ficheros regulados por la legislación de prevención del blanqueo de capitales y de la financiación del terrorismo.
k) Las entidades que desarrollen actividades de publicidad y prospección comercial, incluyendo las de investigación comercial y de mercados, cuando realicen actividades que impliquen la elaboración de perfiles de los mismos.
l) Los centros sanitarios legalmente obligados al mantenimiento de las historias clínicas de los pacientes.

   Excepto, los profesionales de la salud que ejerzan su actividad a título individual.
m) Las entidades que tengan como uno de sus objetos la emisión de informes comerciales que puedan referirse a personas físicas.
n) Los operadores que desarrollen la actividad de juego a través de canales electrónicos, informáticos, telemáticos e interactivos, conforme a la normativa de regulación del juego.

ñ) Las empresas de seguridad privada.

o) Las federaciones deportivas cuando traten datos de menores de edad

El delegado de protección de datos intervendrá en casos de reclamación por los interesados ante las autoridades de protección de datos, ya sea la Agencia Española de Protección de Datos o, las autoridades autonómicas de protección de datos, ya sea:

- Previamente a la interposición de la reclamación, en cuyo caso el delegado de protección de datos comunicará al afectado la decisión que se hubiera adoptado en el plazo máximo de dos meses a contar desde la recepción de la reclamación.
- O una vez interpuesta la reclamación, las autoridades de protección de datos podrán remitir al delegado de protección de datos la reclamación para que este responda a la misma en el plazo de un mes. Si el delegado no responde a la reclamación en plazo indicado, la autoridad de protección de datos competente continuará el procedimiento.

6.5 AUTORIDADES DE CONTROL INDEPENDIENTES EN MATERIA DE PROTECCIÓN DE DATOS

En España, la autoridad de control independiente en materia de protección de datos es la Agencia Española de Protección de Datos (AEPD). Esta entidad tiene la responsabilidad de garantizar el cumplimiento de la normativa de protección de datos y de defender los derechos fundamentales de los ciudadanos en este ámbito. Entidad que se desarrollará en un epígrafe más adelante.

Ley Orgánica 3/2018, de 5 de diciembre, en su artículo 57, establece las funciones y potestades de las autoridades autonómicas de protección de datos en España, en consonancia con el Reglamento (UE) 2016/679 y la normativa autonómica correspondiente. Según el siguiente detalle:

1. Las autoridades autonómicas tienen competencia sobre tratamientos de datos realizados por entidades del sector público de la Comunidad Autónoma o Entidades Locales incluidas en su ámbito territorial, así como por personas físicas o jurídicas en el ejercicio de funciones públicas competentes de la Administración Autonómica o Local, y aquellos tratamientos expresamente previstos en los Estatutos de Autonomía.

2. Estas autoridades pueden emitir circulares con alcance y efectos similares a los establecidos para la Agencia Española de Protección de Datos, en relación con los tratamientos sometidos a su competencia.

7. DERECHOS ARCO Y DERECHOS POL

7.1 DERECHOS ARCO

Toda persona debe poder tener control sobre sus datos personales. Este control se garantiza en la normativa vigente en protección de datos a través de los denominados derechos ARCO (Acceso, Rectificación, Cancelación y Oposición), que están regulados por la Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales y por el Reglamento General de Protección de Datos de 2016 que los incrementó en dos derechos más,

Los derechos ARCO están regulados por la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantías de derechos digitales, (LOPD), en el capítulo II, en los artículos 12 a 18. En ellos se garantizan los diferentes derechos de los cuales disfrutan los usuarios.

Los derechos de los interesados se regulan en los artículos 15 a 22 del Reglamento General de Protección de Datos (RGPD). Aparte de contener los tradicionales derechos ARCO (acceso, rectificación, cancelación y oposición) añade nuevos derechos como son el derecho a la portabilidad del dato, el derecho a la limitación en el tratamiento y el derecho al olvido, como una extensión de los derechos de cancelación y de oposición, así como el derecho a no ser objeto de decisiones individuales automatizadas.

Los derechos ARCO son los derechos que pueden ejercer los ciudadanos sobre sus datos personales y que les dan un mayor control sobre el tratamiento de los mismos; son los derechos de acceso, rectificación, cancelación y oposición.

No existe una ley ARCO como tal, sino que el ejercicio de estos derechos se regula en el Reglamento General de Protección de Datos (RGPD) y en la Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales (LOPD).

El ejercicio de estos derechos de protección de datos es personal. Es decir, en caso de que la solicitud no sea realizada por el titular de los datos, su representante legal o por un representante acreditado, el responsable del fichero puede denegar dicha solicitud.

También deben ejercerse a través de medios sencillos, gratuitos y sujetos a los plazos facilitados por el responsable del fichero.

Todos estos derechos se caracterizan por lo siguiente:

- Su ejercicio es gratuito

- Si las solicitudes son manifiestamente infundadas o excesivas (p. ej., carácter repetitivo) el responsable podrá:
  - Cobrar un canon proporcional a los costes administrativos soportados
  - Negarse a actuar
- Una vez ejercitados, las solicitudes deberán responderse en el plazo de un mes, salvo que sea muy compleja o exista un amplio número de solicitudes, en cuyo caso se puede prorrogar el plazo otros dos meses más
- El responsable está obligado a informar al interesado sobre los medios para ejercitar estos derechos que deberán, además, ser accesibles y no se puede denegar este derecho por el solo motivo de que optes por otro medio
- Si la solicitud se presenta por medios electrónicos, la información se facilitará por estos medios cuando sea posible, salvo que el interesado solicite que sea de otro modo
- 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
- Puedes ejercer los derechos directamente o por medio de tu representante legal o voluntario
- Cabe la posibilidad de que el encargado sea quien atienda tu solicitud por cuenta del responsable si ambos lo han establecido en el contrato o acto jurídico que les vincule

Tras la entrada en vigor del RGPD y la LOPD son denominados derechos ARSULIPO, ya que el derecho de cancelación pasa a ser el derecho de supresión y se añaden los derechos de limitación del tratamiento y portabilidad. Si bien también es posible seguir encontrándolos como derechos ARCOPOL.

En un principio, las siglas ARCO se referían al derecho de Acceso, Rectificación, Cancelación y Oposición. Sin embargo, con la entrada en vigor del RGPD y la LOPD han sido ligeramente modificados. De forma que, se mantienen el derecho de Acceso, Rectificación y Oposición. El derecho de cancelación es sustituido por el derecho de Supresión y el Derecho al Olvido. A su vez, se añaden el Derecho a la Limitación del Tratamiento y la Portabilidad.

En definitiva, en la actualidad estos derechos de protección de datos se resumen en **Acceso**, **Rectificación**, **Supresión (Olvido), Limitación del Tratamiento, Portabilidad y Oposición**. Por ello, la normativa española ha dado en llamarlos derechos **ARSULIPO** o **ARCOPOL**.

7.1.1 Derecho de acceso.

El derecho de acceso está regulado en el artículo 13 de la LOPD y en el artículo 15 del RGPD.

El derecho de acceso es el derecho que se reconoce a los interesados para dirigirse al responsable del tratamiento y conocer así si se están tratando o no sus datos personales y, en caso afirmativo se deberá determinar con qué finalidad, cual es el origen de esos datos y las comunicaciones realizadas o previstas de los mismos.

El interesado tendrá derecho a obtener la siguiente información:

- Copia de los datos personales que están siendo objeto del tratamiento
- Los fines del tratamiento
- La categoría de datos personales que están siendo tratados
- Los destinatarios o categorías de destinatarios a los que se comunicaron o serán comunicados los datos personales, en particular los destinatarios en terceros países u organizaciones internacionales y, este caso, las garantías adecuadas en las que se realizan dichas transferencias
- El plazo previsto de conservación de los datos personales o en caso de no ser posible, los criterios para su determinación
- La existencia del derecho del interesado a solicitar al responsable: la rectificación o supresión de sus datos personales, la limitación del tratamiento de sus datos personales u oponerse a ese tratamiento
- El derecho a presentar una reclamación ante una Autoridad de Control
- Cuando no hayan sido obtenidos directamente del interesado, la información disponible sobre su origen
- La existencia de decisiones automatizadas, incluida la elaboración de perfiles, y al menos en tales casos, información significativa sobre la lógica aplicada, la importancia y las consecuencias previstas de ese tratamiento para el interesado

Cuando se disponga de gran cantidad de información del interesado, el responsable podrá solicitar al interesado, antes de facilitarle la información, que éste especifique la información o actividades de tratamiento a que se refiere su solicitud.

No es necesario que el interesado justifique el ejercicio de este derecho si no se ha ejercido en los últimos 12 meses.

El plazo máximo para la resolución de la solicitud por parte del responsable del fichero es de 30 días desde la recepción de esta.

Tras la comunicación de resolución, el demandante dispondrá de 10 días hábiles para realizar el acceso.

7.1.2 Derecho de rectificación

El derecho de rectificación está regulado en el artículo 14 de la LOPD y en el artículo 16 del RGPD.

El derecho de rectificación es el que permite a la persona afectada solicitar la modificación de datos que sean inexactos o incompletos y a obtener sin dilación indebida del responsable del tratamiento la rectificación de esos datos personales.

En este caso debe justificarse qué datos son los referidos y su corrección, aportando documentación justificativa de la rectificación solicitada.

El responsable del fichero dispone de 10 días hábiles para llevar a cabo la resolución.

7.1.3 Derecho de cancelación

El derecho de supresión está regulado en el artículo 15 de la LOPD y en el artículo 17 del RGPD.

Es el derecho que tiene el interesado a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernen y que estará obligado a suprimir cuando concurra alguna de las circunstancias siguientes:

a) Los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo;
b) El interesado retire el consentimiento en que se basa el tratamiento de conformidad con el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), y este no se base en otro fundamento jurídico;
c) El interesado se oponga al tratamiento con arreglo al artículo 21, apartado 1, y no prevalezcan otros motivos legítimos para el tratamiento, o el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 2;
d) Los datos personales hayan sido tratados ilícitamente;

e) Los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento;
f) Los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información mencionados en el artículo 8, apartado 1.

El derecho de cancelación es aquel por el cual el afectado puede solicitar la supresión de los datos que resulten inadecuados o excesivos, sin perjuicio del deber de bloqueo. Debe indicarse el dato a cancelar y el motivo, aportando documentación justificativa de la rectificación solicitada y el responsable del fichero dispone de 10 días hábiles para llevar a cabo la resolución.

7.1.4 Derecho de oposición

Se trata del derecho de una persona a oponerse al tratamiento de sus datos personales. El derecho de oposición está regulado en el artículo 18 de la LOPD y en los artículos 21 y 22 del RGPD.

Este derecho está recogido en el artículo 21 del RGPD y otorga a los individuos la capacidad de oponerse al procesamiento de sus datos personales en determinadas circunstancias. Principalmente, una persona puede ejercer su derecho de oposición en situaciones donde el tratamiento de sus datos se basa en intereses legítimos del responsable del tratamiento o en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos. En tales casos, el responsable del tratamiento debe cesar el procesamiento a menos que pueda demostrar motivos legítimos imperiosos que prevalezcan sobre los intereses, derechos y libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones.

Además, el interesado tendrá derecho de oposición en todo momento cuando se trate de marketing directo. Es decir, una persona puede oponerse en cualquier momento al procesamiento de sus datos personales con fines de mercadotecnia, y en tal caso, el responsable del tratamiento debe cesar inmediatamente dicho procesamiento.

El derecho de oposición también incluye el uso de datos personales para la elaboración de perfiles en la medida en que esté relacionado con el marketing directo. En el caso de que el interesado ejercite este derecho, los datos personales ya no serán tratados para dichos fines.

Para ejercer el derecho de oposición, el interesado debe comunicar su decisión al responsable del tratamiento, quien tiene la obligación de atender dicha solicitud a menos que se apliquen excepciones específicas mencionadas anteriormente (interés público o en el ejercicio de poderes públicos que prevalezcan sobre los intereses, derechos y libertades de los interesados).

Este derecho garantiza a los individuos un control significativo sobre cómo y cuándo se utilizan sus datos personales, reforzando así la protección de la privacidad y la autodeterminación informativa en el ámbito digital.

7.2 DERECHOS POL (RGPD)

Como anteriormente se comentó, la nueva normativa amplia los derechos ARCO para adaptarlos a la nueva realidad digital.

7.2.1. Derecho a la portabilidad de los datos

El derecho a la portabilidad de los datos es uno de los derechos fundamentales contemplados en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016.

Este derecho, descrito en el artículo 20 del RGPD, permite a los interesados recibir los datos personales que han proporcionado a un responsable del tratamiento en un formato estructurado, de uso común y lectura mecánica. Además, tienen el derecho de transmitir esos datos a otro responsable del tratamiento sin impedimentos por parte del responsable al que se los proporcionaron.

a) Elementos clave del derecho a la portabilidad

1. Aplicabilidad: este derecho se aplica cuando el tratamiento de datos se basa en el consentimiento del interesado o en la necesidad de ejecutar un contrato, y cuando el tratamiento se lleva a cabo por medios automatizados.

2. Alcance: incluye únicamente los datos personales que el interesado ha proporcionado al responsable del tratamiento. Esto puede abarcar datos explícitamente suministrados por el interesado, así como datos observados sobre él, como información generada a través del uso de un servicio o dispositivo.

3. Entrega de datos: los datos deben ser proporcionados en un formato estructurado, de uso común y lectura mecánica, como archivos CSV o XML, lo que facilita su transferencia a otro sistema.

4. Transmisión directa: siempre que sea técnicamente posible, el interesado puede solicitar que los datos sean transmitidos directamente de un responsable del tratamiento a otro.

b) Propósito y beneficios

El derecho a la portabilidad de los datos está diseñado para aumentar el control y la capacidad de los individuos sobre su propia información personal. Facilita la transición entre diferentes proveedores de servicios y promueve una mayor competencia en el mercado, al reducir las barreras de salida para los usuarios que desean cambiar de servicio.

c) Límites y consideraciones

El ejercicio del derecho a la portabilidad no debe afectar negativamente los derechos y libertades de otros. Por ejemplo, si la transmisión de datos implica revelar información personal de terceros, el responsable del tratamiento debe tomar las medidas necesarias para proteger esos datos.

d) Ejercicio del derecho

Para ejercer el derecho a la portabilidad, el interesado debe presentar una solicitud al responsable del tratamiento. Este último tiene la obligación de responder a la solicitud sin demora indebida y, en cualquier caso, en el plazo de un mes desde su recepción, plazo que puede prorrogarse otros dos meses en casos de solicitudes complejas o numerosas.

7.2.2. Derecho de supresión “el derecho al olvido”

El derecho de supresión, también conocido como derecho al olvido, está establecido en el Reglamento General de Protección de Datos (RGPD) de la Unión Europea, específicamente en su artículo 17. Este derecho permite a los individuos solicitar la eliminación de sus datos personales cuando se cumplen ciertas condiciones.

Según el RGPD, los usuarios tienen derecho a solicitar la supresión de sus datos personales si se cumplen alguno de los siguientes motivos:

1. Los datos personales ya no son necesarios para los fines para los cuales fueron recogidos o tratados de otro modo.

2. La persona retira el consentimiento en el cual se basa el tratamiento de conformidad.
3. Datos personales hayan sido tratados ilícitamente.
4. Los datos personales deban suprimirse para el cumplimiento de una obligación legal de la Unión Europea o en los Estados miembros.
5. Los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información.

Hay excepciones al derecho de supresión:

El derecho de supresión no es absoluto y puede haber circunstancias en las que no se aplique, por ejemplo, cuando el procesamiento es necesario para el ejercicio del derecho a la libertad de expresión e información, para el cumplimiento de una obligación legal que requiera el tratamiento según la ley de la Unión o de los Estados miembros a los que esté sujeto el responsable del tratamiento, para la realización de una tarea realizada en interés público o en el ejercicio de la autoridad oficial conferida al responsable del tratamiento, o por razones de interés público en el ámbito de la salud pública.

El derecho a la supresión concretado en “el derecho al olvido”, es una de las mayores novedades de este reglamento, y está enfocado a ámbitos digitales. Asimismo, es la versión mejorada y con más peso que el derecho de cancelación. Este nuevo derecho introducido en el RGPD sirve para tener el pleno derecho a pedir a las compañías que eliminen nuestros datos, siempre y cuando estos estén basados en nuestro consentimiento.

Cuando un individuo ejerce su derecho de supresión, el responsable del tratamiento debe tomar medidas razonables, incluidas las técnicas, para informar a otros controladores que están procesando los datos personales que el sujeto de datos ha solicitado la eliminación de cualquier enlace a esos datos, o cualquier copia o réplica de esos datos.

En resumidas cuentas, cuando antes los usuarios se negaban a que las compañías tratasen sus datos, ahora estas deben ceder y borrar los datos del usuario; si este pide su eliminación, no podrán seguir guardando esos datos.

Tanto el derecho de cancelación como el derecho al olvido, forman parte del derecho a la supresión, ya que este engloba más ámbitos.

7.2.3 Derecho a la limitación del tratamiento

Cualquier persona tiene derecho a exigir al responsable del tratamiento la limitación del tratamiento de sus datos personales siempre que se dé alguna de las siguientes condiciones:

- Cuando el interesado impugne la exactitud de los datos, durante el tiempo necesario para que el responsable verifique la información.
- Si el tratamiento de datos es ilícito, pero el interesado decide hacer uso de su derecho a la limitación del tratamiento en lugar del derecho a la supresión.
- En caso de que el responsable ya no necesite esos datos para los fines para los que fueron recabados, pero el interesado sí los necesite para el ejercicio o formulación de reclamaciones.
- Cuando la persona haya ejercicio su derecho de oposición, durante el tiempo necesario para verificar si los motivos del responsable prevalecen sobre el derecho del interesado.

Cuando se haya aplicado la limitación del tratamiento en virtud de los supuestos anteriores, los datos solo podrán ser objeto de tratamiento con el consentimiento del interesado, para el ejercicio o defensa de reclamaciones o para la protección de los derechos de otra persona.

Según el Reglamento General de Protección de Datos (RGPD) 2016/679, hay varias limitaciones al tratamiento de datos personales que deben ser respetadas por las organizaciones y entidades que manejan dichos datos. Aquí algunas de las principales limitaciones:

1. Principio de Finalidad Limitada: los datos personales deben ser recogidos con fines específicos, explícitos y legítimos, y no pueden ser tratados de manera incompatible con esos fines.
2. Minimización de Datos: los datos personales deben ser adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.
3. Exactitud de los Datos: los datos personales deben ser precisos y, si es necesario, actualizados; se deben tomar todas las medidas razonables para garantizar que los datos inexactos sean rectificados o suprimidos sin demora.
4. Limitación del Almacenamiento: los datos personales deben ser mantenidos de manera que permita la identificación de los interesados durante no más tiempo del necesario para los fines para los que son tratados.

5. Integridad y Confidencialidad: los datos personales deben ser tratados de tal manera que se garantice una seguridad adecuada, incluida la protección contra el tratamiento no autorizado o ilegal y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas.
6. Principio de Responsabilidad Proactiva: el responsable del tratamiento es responsable de demostrar que se cumplen los principios de protección de datos.
7. Limitaciones específicas para categorías especiales de datos: el tratamiento de categorías especiales de datos personales (como datos de salud, origen étnico, opiniones políticas, etc.) está sujeto a restricciones adicionales y solo puede realizarse bajo condiciones específicas.

Estas limitaciones buscan garantizar que el tratamiento de datos personales se realice de manera justa, transparente y segura, respetando en todo momento los derechos de los individuos cuyos datos están siendo procesados.

7.3 SANCIONES POR EL INCUMPLIMIENTO DE LOS DERECHOS ARCO Y POL

El Reglamento 2016/679 del Parlamento Europeo y del Consejo (RGPD), establece un marco regulatorio para la protección de datos personales en la Unión Europea. En cuanto al incumplimiento de los derechos ARCO (Acceso, Rectificación, Cancelación y Oposición) y POL (Portabilidad, Oposición y Limitación), el RGPD contempla sanciones específicas en caso de infracción.

Las sanciones por incumplimiento del RGPD pueden variar dependiendo de la gravedad de la infracción y pueden incluir:

1. Advertencias y apercibimientos: en casos menos graves, las autoridades de protección de datos pueden emitir advertencias o apercibimientos a los responsables del tratamiento de datos que no cumplan con las disposiciones del RGPD. Estas advertencias suelen ser el primer paso antes de imponer sanciones más severas.

2. Multas administrativas: las multas pueden ser significativas y se aplican en función de la naturaleza de la infracción. El RGPD permite multas de hasta el 4% del volumen de negocio global anual del año financiero anterior o hasta 20 millones de euros (el importe que resulte mayor) para las infracciones más graves. Para infracciones menos

graves, las multas pueden ser de hasta el 2% del volumen de negocio global anual o hasta 10 millones de euros.

3. Medidas correctivas y restricciones en el tratamiento de datos: además de las multas, las autoridades de protección de datos pueden ordenar la adopción de medidas correctivas, como la rectificación, supresión o limitación del tratamiento de los datos personales afectados por la infracción.

Es importante tener en cuenta que las autoridades de protección de datos de cada país de la UE son responsables de imponer las sanciones y adoptar las medidas adecuadas en caso de incumplimiento del RGPD. La gravedad de la infracción, la naturaleza de los datos afectados y las circunstancias específicas del caso influirán en la determinación de la sanción específica que se aplique.

8. LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

La Agencia Española de Protección de Datos (AEPD) es la autoridad de control independiente que vela por el cumplimiento de la normativa sobre protección de datos en España. Su misión principal es garantizar y proteger, en lo que respecta al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente su honor e intimidad personal y familiar.

8.1 HISTORIA, EVOLUCIÓN Y MARCO NORMATIVO

La AEPD fue creada en 1992 mediante la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal (LORTAD). Esta ley estableció las bases para la protección de datos personales en España, en consonancia con la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

La Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal, encomendó el control de la aplicación de sus disposiciones a un ente público independiente al que denominó Agencia de Protección de Datos y que se caracterizaba por la absoluta independencia de su director en el ejercicio de sus funciones, reforzada por el establecimiento de un mandato fijo que solo podía ser acortado por un numerus clausus de causas de cese. La efectiva creación de la Agencia se llevó a cabo mediante la regulación de su estructura orgánica y la aprobación de su Estatuto por el Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos.

Posteriormente, la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, aprobada para transponer a nuestro Derecho la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, mantuvo la configuración de la Agencia como un ente de derecho público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las Administraciones públicas en el ejercicio de sus funciones.

Con el tiempo, la AEPD ha evolucionado para adaptarse a los cambios tecnológicos y legislativos. En 2018, la entrada en vigor del Reglamento General de Protección de Datos (RGPD) de la Unión Europea supuso un cambio significativo en el marco legal de la protección de datos, lo que llevó a la actualización de la normativa española a través de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPD). Por otro lado, hay que tener en cuenta que la Agencia Española de Protección de Datos no solo ejerce las competencias derivadas del Reglamento, sino que también ejercerá las que establece la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales. Igualmente ejerce actualmente las potestades derivadas de la Directiva 2002/58 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, que en la actualidad se recogen en la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, y en la legislación en materia de telecomunicaciones.

Por todo ello, resulta necesario la aprobación de un nuevo Estatuto que adapte la organización y funcionamiento de la Agencia Española de Protección de Datos a lo previsto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y en la Ley Orgánica 3/2018, de 5 de diciembre. Así surge el actual Estatuto de la Agencia Española de Protección de Datos, aprobado por el Real Decreto 389/2021, de 1 de junio, por el que se aprueba el Estatuto de la Agencia Española de Protección de Datos, y deroga el anterior Estatuto de la AGPD aprobado por el Real Decreto 428/1993, de 26 de marzo

Actualmente está en vigor el Real Decreto 389/2021, de 1 de junio, por el que se aprueba el Estatuto de la Agencia Española de Protección de Datos, que derogó el anterior Real Decreto 428/1993, de 26 de marzo por el que se creó el Estatuto de la Agencia de Protección de Datos y suprime los siguientes órganos directivos:

a) El Director de la Agencia Española de Protección de Datos
b) El Registro General de Protección de Datos.
c) La Inspección de Datos

El marco legal de la Agencia Española de Protección de Datos se rige principalmente por el Reglamento General de Protección de Datos (RGPD) y la Ley Orgánica de

Protección de Datos y Garantía de Derechos Digitales (LOPD). El RGPD, que entró en vigor el 25 de mayo de 2018, establece un marco legal uniforme para la protección de datos en toda la UE, y la LOPDGDD adapta y complementa el RGPD en el contexto español, abordando aspectos específicos y estableciendo derechos adicionales para los ciudadanos.

Los ciudadanos tienen varios derechos en relación con sus datos personales, que la AEPD se encarga de proteger, son los siguientes:

1. Derecho de acceso: permite a los individuos conocer y obtener información sobre sus datos personales tratados.
2. Derecho de rectificación: permite corregir datos personales inexactos o incompletos.
3. Derecho de supresión (derecho al olvido): permite solicitar la eliminación de datos personales cuando ya no sean necesarios o si se ha retirado el consentimiento.
4. Derecho a la limitación del tratamiento: permite restringir el tratamiento de los datos personales en ciertas circunstancias.
5. Derecho a la portabilidad de los datos: permite recibir los datos personales facilitados y transmitirlos a otro responsable del tratamiento.
6. Derecho de oposición: permite oponerse al tratamiento de los datos personales por motivos relacionados con su situación particular.

8.2 FUNCIONES Y COMPETENCIAS

La Agencia Española de Protección de Datos (AEPD) es la autoridad independiente encargada de velar por el cumplimiento de la legislación sobre protección de datos en España. Sus funciones y competencias están definidas principalmente en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPD), así como en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento General de Protección de Datos, RGPD).

Las funciones de la AEPD son las siguientes:

1. Control y Supervisión del Cumplimiento:

   - Supervisar y garantizar la aplicación de la normativa de protección de datos.
   - Realizar inspecciones y auditorías para verificar el cumplimiento de la ley.

2. Atención de Reclamaciones y Consultas:

   - Atender las reclamaciones presentadas por los interesados.
   - Asesorar a ciudadanos y empresas sobre sus derechos y obligaciones en materia de protección de datos.

3. Promoción y Difusión:

   - Promover la concienciación y formación en materia de protección de datos.
   - Fomentar buenas prácticas y elaborar guías y recomendaciones.

4. Sanciones y Medidas Correctivas:

   - Imponer sanciones administrativas en caso de infracciones.
   - Adoptar medidas correctivas para asegurar el cumplimiento de la normativa.

5. Colaboración Internacional:

   - Colaborar con otras autoridades de protección de datos a nivel europeo e internacional.
   - Participar en el Comité Europeo de Protección de Datos (EDPB).

6. Investigación y Desarrollo:

   - Realizar estudios e investigaciones en el ámbito de la protección de datos.
   - Promover la innovación tecnológica respetuosa con la privacidad.

7. Autorizar Transferencias Internacionales de Datos:

   - Evaluar y autorizar, cuando sea necesario, transferencias internacionales de datos personales.

Las competencias de la AEPD son las siguientes:

1. Poder de Investigación:

   - Investigar posibles infracciones de la normativa de protección de datos.
   - Requerir información a las entidades responsables del tratamiento de datos.

2. Poder de Corrección:

   - Emitir advertencias y apercibimientos.
   - Ordenar la rectificación, limitación o supresión de datos.
   - Prohibir o suspender temporalmente tratamientos de datos.

3. Poder de Asesoramiento:

   - Asesorar al Gobierno y otras entidades sobre cuestiones relativas a la protección de datos.
   - Emitir informes y dictámenes preceptivos en el ámbito de la protección de datos.

4. Poder Normativo:

   - Elaborar y proponer normativa en materia de protección de datos.
   - Desarrollar instrucciones y criterios de interpretación de la normativa.

La AEPD desempeña un papel crucial en la protección de los derechos fundamentales de los ciudadanos en relación con sus datos personales, garantizando que se manejan de manera segura y conforme a la legislación vigente.

8.3 RECURSOS Y HERRAMIENTAS

La Agencia Española de Protección de Datos (AEPD) proporciona una serie de recursos y herramientas para ayudar a las organizaciones y ciudadanos a cumplir con la legislación vigente en materia de protección de datos personales. Estos recursos y herramientas están diseñados para facilitar el cumplimiento de la normativa vigente y asegurar una adecuada protección de los datos personales en España.

A continuación, se detallan algunos de los recursos y herramientas más importantes que ofrece la AEPD:

1. Guías y Manuales.

- Guía del Reglamento General de Protección de Datos (RGPD): proporciona una explicación detallada del RGPD, incluyendo sus principios, derechos de los interesados, obligaciones de los responsables y encargados del tratamiento, y medidas de seguridad.
- Guía sobre el uso de cookies: orienta sobre el uso de cookies en sitios web y cómo cumplir con las obligaciones de información y obtención de consentimiento.
- Guía de seguridad para responsables de tratamiento de datos: ofrece recomendaciones sobre medidas de seguridad técnicas y organizativas para proteger los datos personales.

2. Herramientas de Evaluación

- Facilita_RGPD: herramienta para ayudar a pequeñas y medianas empresas a cumplir con el RGPD mediante un cuestionario que genera informes personalizados con recomendaciones.
- EIPD: herramienta para la Evaluación de Impacto en la Protección de Datos, que ayuda a identificar y mitigar riesgos en los tratamientos de datos personales.

3. Modelos y Plantillas

- Modelos de contratos de encargado del tratamiento: plantillas para formalizar contratos entre responsables y encargados del tratamiento conforme al RGPD.
- Formularios de ejercicio de derechos: plantillas para que los ciudadanos puedan ejercer sus derechos de acceso, rectificación, supresión, limitación del tratamiento, portabilidad y oposición.

4. Canal Prioritario

- Canal Prioritario: mecanismo para la denuncia de la difusión ilícita de contenidos sensibles en Internet, facilitando su retirada rápida.

5. Formación y Concienciación

- Cursos y webinars: Ofrecen formación sobre protección de datos para diferentes niveles de conocimiento y sectores.
- Material educativo: Incluye folletos, vídeos y presentaciones para sensibilizar a ciudadanos y organizaciones sobre la importancia de la protección de datos.

6. Asesoramiento y Consultas

- Consultas jurídicas: Servicio de atención a consultas sobre la aplicación de la normativa de protección de datos.
- Informes y resoluciones: Base de datos con informes y resoluciones emitidas por la AEPD sobre distintos aspectos de la normativa.

9. LA DELEGACIÓN DE PROTECCIÓN DE DATOS DE LA GENERALITAT VALENCIANA

La Delegación de Protección de Datos de la Generalitat Valenciana es un organismo encargado de garantizar el cumplimiento de las normativas sobre protección de datos en la Comunidad Valenciana.

Su misión principal es asegurar que las instituciones y entidades públicas y privadas que operen en nuestro ámbito territorial cumplan con las leyes de privacidad, garantizando así los derechos fundamentales de los ciudadanos en relación con el tratamiento de sus datos personales.

9.1 CREACIÓN Y MARCO NORMATIVO

La Delegación de Protección de Datos de la Generalitat fue creada por el Decreto 195/2018, de 31 de octubre de 2018, del Consell, siendo única para todas las consellerias y entidades del sector público instrumental de la administración de la Generalitat Valenciana.

La persona titular de la Delegación de protección de datos tiene rango de subdirector general y depende orgánicamente de la Subsecretaría de la Presidencia de la Generalitat. Los titulares de las Subdelegaciones adjuntas tienen rango de dirección de servicio.

El Delegado o Delegada de Protección de Datos y las subdelegaciones adjuntas ejercen sus funciones con total independencia, prestando la debida atención a los riesgos asociados a las operaciones de tratamiento de datos de carácter personal y teniendo en cuenta la naturaleza, el alcance, el contexto y los fines de los tratamientos.

9.2 FUNCIONES DEL DELEGADO O DELEGADA DE PROTECCIÓN DE DATOS

El Decreto 195/2018, de 31 de octubre de 2018, del Consell, le asigna al Delegado o Delegada de Protección de Datos las atribuciones siguientes:

a) Informar y asesorar a las personas responsables o encargadas del tratamiento en la Administración de la Generalitat y su sector público instrumental, y al personal que lleve a cabo tratamientos de datos, de las obligaciones que los incumben en relación con la

normativa de protección de datos personales, en particular sobre la obligación de llevar un registro de actividades de tratamiento.

b) Supervisar el cumplimiento de lo que prevé la normativa de protección de datos y las políticas de la Administración de la Generalitat y su sector público instrumental en esta materia.
c) Proporcionar el asesoramiento necesario en relación con las evaluaciones de impacto en la protección de datos y supervisar su aplicación en conformidad con el artículo 35 del RGPD.
d) Cooperar con la autoridad de control (Agencia Española de Protección de Datos).
e) Actuar como punto de contacto de la autoridad de control en cuestiones relacionadas con los tratamientos, incluyendo la consulta previa a que se refiere el artículo 36 del RGPD.
f) Realizar consultas a la autoridad de control, si es el caso, sobre cualquier otro asunto.
g) Emitir recomendaciones a las personas responsables o encargadas del tratamiento en materia de protección de datos.
h) Asegurar que las violaciones de la seguridad de los datos sean notificadas a las autoridades.
i) Elaboración de un informe anual de las actividades realizadas y sus conclusiones.
j) Cualesquiera otras funciones que le atribuya la normativa en materia de protección de datos.

La Orden 1/2021, de 20 de abril, de la consellera de Participación, Transparencia, Cooperación y Calidad Democrática, por la que se desarrolla el Decreto 179/2020, de 30 de octubre, del Consell, por el cual se aprueba el Reglamento orgánico y funcional de la Conselleria de Participación, Transparencia, Cooperación y Calidad Democrática, del Consell, asigna a la persona titular de la Delegación de Protección de Datos las atribuciones siguientes:

a) Informar y asesorar a las personas responsables o encargadas del tratamiento en la Administración de la Generalitat y su sector público instrumental, y el personal que lleve a cabo tratamientos de datos, de las obligaciones que los incumben en relación con la normativa de protección de datos personales, en particular sobre la obligación de llevar un registro de actividades de tratamiento.

b) Supervisar el cumplimiento de lo previsto en la normativa de protección de datos y las políticas de la Administración de la Generalitat y su sector público instrumental en esta materia.
c) Inspeccionar los procedimientos relacionados con la protección de datos de carácter personal.
d) Proporcionar el asesoramiento necesario en relación con las evaluaciones de impacto en la protección de datos y supervisar su aplicación en conformidad con el artículo 35 del Reglamento general de protección de datos.
e) Cooperar con la autoridad de control.
f) Actuar como punto de contacto de la autoridad de control en cuestiones relacionadas con los tratamientos, incluyendo la consulta previa a que se refiere el artículo 36 del Reglamento general de protección de datos.
g) Actuar como punto de contacto con las personas interesadas por lo que respecta a todas las cuestiones relativas al tratamiento de sus datos personales y al ejercicio de sus derechos.
h) Atender las reclamaciones en materia de protección de datos efectuados directamente por las personas interesadas o remesas por la autoridad de control de acuerdo con lo establecido en el artículo 37 de la Ley orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales.
i) Realizar consultas a la autoridad de control, en su caso, sobre cualquier otro asunto.
j) Emitir recomendaciones a las personas responsables o encargadas del tratamiento en materia de protección de datos.
k) Asegurar que las violaciones de la seguridad de los datos sean notificadas a las autoridades, en coordinación con las personas responsables en materia de seguridad de la información.
l) Elaboración de un informe anual de las actividades realizadas y sus conclusiones.
m) Cualesquiera otras funciones que le atribuya la normativa en materia de protección de datos

Los centros docentes y sanitarios titularidad de la administración de la Generalitat y su sector público instrumental están incluidos en el ámbito de competencia del delegado o delegada de protección de datos.

9.3 SUBDELEGACIONES ADJUNTAS Y FUNCIONES

Para el cumplimiento, desarrollo y ejecución de sus funciones, el/la delegado/a o delegada de protección de datos cuenta con tres subdelegaciones de protección de datos adjuntos:

1. Subdelegación de Protección de Datos de la Administración de la Generalitat.
2. Subdelegación de Protección de Datos del sector público instrumental.
3. Subdelegación de Protección de Datos sanidad y educación.

En cuanto a las funciones de los/as subdelegados/as de protección de datos, la mencionada Orden 1/2021, de 20 de abril, de la consellera de Participación, Transparencia, Cooperación y Calidad Democrática, atribuye a los/as subdelegados/as de protección de datos las siguientes funciones:

a) Pedir información e identificar las actividades de tratamiento de datos en colaboración con las personas responsables o encargadas del tratamiento y el empleado que lleve a cabo el tratamiento.
b) Analizar y comprobar la conformidad con la normativa de las actividades de tratamiento.
c) Asesorar y supervisar, entre otras, en las áreas siguientes:
    1. Cumplimiento de principios relativos al tratamiento, como los de limitación de finalidad, minimización o exactitud de los datos.
    2. Identificación de las bases jurídicas de los tratamientos.
    3. Valoración de compatibilidad de finalidades diferentes de las que originaron lo recoge inicial de los datos.
    4. Determinación de la existencia de normativa sectorial que pueda exigir condiciones de tratamiento específicas.
    5. Diseño e implantación de medidas de información a las personas afectadas por los tratamientos de datos.
    6. Establecimiento de mecanismos de recepción y gestión de las solicitudes de ejercicio de derechos por parte de las personas interesadas**.**
    7. Valoración de las solicitudes de ejercicio de derechos por parte de las personas interesadas.
    8. Contratación de personas encargadas de tratamiento, incluido el contenido de los contratos o actos jurídicos que regulan la relación responsable-persona encargada.

9. Identificación de los instrumentos de transferencia internacional de datos adecuados a las necesidades y características de la organización y de las razones que justifican la transferencia.
10. Diseño e implantación de políticas de protección de datos.
11. Auditoría de protección de datos.
12. Análisis de riesgo de los tratamientos realizados.
13. Implantación de las medidas de protección de datos desde el diseño y protección de datos por defecto adecuadas a los riesgos y naturaleza de los tratamientos.
14. Implantación de las medidas de seguridad adecuadas a los riesgos y naturaleza de los tratamientos.
15. Establecimiento de procedimientos de gestión de violaciones de seguridad de los datos, incluida la evaluación del riesgo para los derechos y libertades de las personas afectadas y los procedimientos de notificación a las autoridades de supervisión y a las personas afectadas.
16. Determinación de la necesidad de realización de evaluaciones de impacto sobre la protección de datos.
17. Realización de evaluaciones de impacto sobre la protección de datos.
18. Implantación de programas de formación y sensibilización del personal en materia de protección de datos.

d) Cualquier otra que se los encomiendo en relación con las materias que los son propias.

9.4 EJERCICIO DE DERECHOS Y RECLAMACIONES

El derecho a la protección de datos supone la capacidad de las personas interesadas a ejercer un control sobre sus datos personales; este control pueden ejercerlo solicitando el acceso, la rectificación y supresión de sus datos de carácter personal, así como solicitando el derecho de oposición y limitación de los tratamientos de sus datos de carácter personal.

Estos derechos están regulados en los artículos 15 y siguientes del RGDP, así como en los artículos 13 y siguientes de la LOPD (desarrollados en el epígrafe 7 de este trabajo):

- Derecho de acceso: regulado en el artículo 15 RGPD y en el artículo 13 de la LO 3/2018. La persona interesada tendrá derecho a obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que la conciernen y, en este caso, derecho de acceso a los datos personales.
- Derecho de rectificación: regulado en los artículos 16 y 19 del RGPD y en el artículo 14 de la LO 3/2018. La persona interesada tendrá derecho a obtener sin más dilación indebida de la entidad responsable del tratamiento la rectificación de los datos personales inexactos que le conciernan.
- Derecho de supresión o derecho al olvido: regulado en el artículo 17 y 19 del RGPD y en el artículo 15 de la LO 3/2018. La persona interesada tendrá derecho a obtener del responsable del tratamiento la supresión de los datos personales que le conciernan, la cual estará obligada a suprimir sin más dilación indebida los datos personales cuando concurra alguna de las circunstancias señaladas en la normativa citada.
- Derecho de limitación: regulado en el artículo 18 del RGPD y el artículo 16 de la LO 3/2018. La persona interesada tendrá derecho a obtener del responsable del tratamiento la limitación del tratamiento de los datos cuando se cumpla alguna de las condiciones señaladas en la normativa citada.
- Derecho de oposición: regulado en el artículo 21 del RGPD y en el artículo 18 de la LO 3/2018. La persona interesada tendrá derecho a oponerse en cualquier momento, por motivos relacionados con su situación particular, al hecho que datos personales que lo conciernan sean objeto de un tratamiento, en los términos señalados en la normativa citada.

El responsable del tratamiento está obligado a resolver la solicitud de la persona interesada sin más dilación indebida y a más tardar en el plazo de un mes desde su recepción, aunque, si se tiene en cuenta la complejidad y número de solicitudes, se puede prorrogar el plazo otros dos meses más.

Transcurrido el plazo sin que de manera exprés se responda a la petición, la persona interesada podrá interponer la **reclamación** prevista en el artículo 37 de la Ley Orgánica 3/2018, de 5 de diciembre de protección de datos personales y garantía de derechos digitales.

Las personas afectadas podrán presentar una reclamación, bien ante la Delegación de Protección de Datos de la Generalitat bien ante la autoridad de control competente, en

nuestro caso la Agencia Española de Protección de Datos, en los supuestos en los cuales no haya sido atendida su solicitud de ejercicio de derechos o se haya producido una posible infracción del que se dispone en la normativa de protección de datos por parte de la Administración del Consell o su sector público instrumental.

Cuando una reclamación se presente ante la Delegación de Protección de Datos, de acuerdo con el artículo 37.1 de la Ley Orgánica 3/2018, de 5 de diciembre, esta tendrá que notificar a la persona reclamante la decisión adoptada en el plazo de dos meses.

Respondida la reclamación por la Delegación de Protección de Datos, en caso de disconformidad, la persona afectada podrá presentar una reclamación ante la Agencia Española de Protección de Datos, en los términos establecidos en la Ley Orgánica 3/2018, de 5 de diciembre.

9.5 PRINCIPIOS DE ACTUACIÓN GENERAL BAJO LOS CUALES HAN DE ACTUAR LOS RESPONSABLES

La actuación de los responsables del tratamiento tiene que responder a los principios regulados en el artículo 5 del RGPD, y que se constituyen en auténticas obligaciones:

a) Principio de licitud

Los responsables del tratamiento en la Generalitat podrán tratar datos de carácter personal si disponen de alguna de las siguientes bases de legitimación (artículo 6 del RGPD):

- Que tengan el consentimiento de la persona afectada para una o varias finalidades específicas (el consentimiento es de carácter excepcional en las administraciones públicas).
- Que sea necesario para ejecutar un contrato en que la persona interesada es parte, o para aplicar medidas precontractuales a petición de la persona interesada.
- Que sea necesario para cumplir una obligación legal del responsable del tratamiento.
- Que sea necesario para proteger intereses vitales de la persona interesada o de otra persona física.
- Que sea necesario para cumplir una misión realizada en interés público o en el ejercicio de poderes públicos otorgados a la persona responsable del tratamiento.

El tratamiento de categorías especiales de datos personales (datos genéticos, datos biométricos, de salud, datos relativos a la vida sexual o que revelan el origen étnico, racional, las opiniones políticas, las convicciones religiosas o filosóficas o la afiliación sindical) solo está permitido en las circunstancias previstas en el artículo 9 RGPD.

b) Principio de transparencia

Este principio tiene que aplicarse a lo largo de todo el proceso de tratamiento de los datos de carácter personal. La información a las personas interesadas se tiene que proporcionar de manera concisa, transparente, inteligible y de fácil acceso, en un lenguaje claro y o sencillo.

Los responsables tienen la obligación de informar a las personas afectadas de los siguientes aspectos:

- La identidad y los datos de contacto del responsable.
- Los datos del delegado/ada de protección de datos.
- Los fines del tratamiento a que se destinan los datos personales.
- Las personas destinatarias o las categorías de los datos personales de personas destinatarias, si es el caso.
- La intención de transferir los datos en un tercer país o a una organización internacional y la base para realizarlo.
- El plazo durante el cual se conservarán los datos.
- La existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos a la persona interesada, y su rectificación y supresión, o la limitación de su tratamiento o a oponerse a este.
- El derecho a retirar en cualquier momento el consentimiento que se ha prestado.
- El derecho a presentar una reclamación ante una autoridad de control.
- Si la comunicación de datos es un requisito legal o contractual o un requisito necesario para subscribir un contrato
- La existencia de decisiones automatizadas, incluidas la lógica aplicada y sus consecuencias.

c) Principio de minimización y proporcionalidad

Los responsables recogerán únicamente aquellos datos que sean adecuadas, pertinentes y limitadas a las finalidades para los cuales son tratadas

d) Principio de exactitud de los datos

Los datos tienen que estar actualizadas y ser exactos. Por este motivo, los responsables adoptarán todas las medidas razonables porque se supriman o rectifican sin más dilación aquellos datos que sean inexactos respecto a los fines para los cuales se tratan.

e) Principio de limitación en la conservación

Los responsables tendrán que conservar los datos durante el tiempo necesario para los fines del tratamiento. Solo podrán conservarse durante periodos más largos con fines de archivo, interés público, investigación científica o histórica o hasta estadísticos.

f) Principio de seguridad e integridad

El análisis del riesgo requiere de una evaluación por tratamiento, que tendrá que hacerse a través de uno de los siguientes instrumentos: el análisis de riesgos o la evaluación de impacto (este último en caso de que el tratamiento comporto un alto riesgo).

g) Principio de confidencialidad:

Los responsables están sujetos al deber de confidencialidad. Esta obligación es complementaria al deber de secreto profesional. Estas obligaciones se mantendrán aunque haya finalizado la relación del obligado con el responsable.

h) Principio de responsabilidad proactiva

Es principio que supone la obligación del responsable de cumplir los principios de protección de datos establecidos en el art. 5.1 del RGPD y la capacidad de demostrar este cumplimiento. Cada responsable tiene que determinar las medidas técnicas y organizativas necesarias para cumplir la normativa en materia de protección de datos.

9.6 OTRAS OBLIGACIONES DE LAS PERSONAS RESPONSABLES.

a) RESPONSABLES DEL TRATAMIENTO

1. **Registro de actividades de tratamiento**

Los responsables tienen que llevar un Registro de las Actividades de Tratamiento (RAT) de su organización. Este registro tiene que contener, respecto de cada actividad, la información que establece el artículo 30 del RGPD:

- Nombre y datos de contacto de la entidad responsable y, si es el caso, la corresponsable, así como del Delegado/ada de Protección de Datos, si hay.
- Finalidades del tratamiento.
- Descripción de categorías de personas interesadas y categorías de datos personales tratados.
- Transferencias internacionales de datos.
- Cuando sea posible, plazos previstos para suprimir los datos.
- Cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad.

2. Notificación de las violaciones de seguridad de los datos personales/brechas de datos personales

Los responsables tienen que notificar las violaciones de la seguridad de los datos personales que se produzcan a la autoridad de control. Esta notificación se realizará sin más dilación indebida y, si es posible, en un plazo máximo de 72 horas desde que tengan constancia, salvo que sea improbable que constituya un riesgo para los derechos y las libertades de las personas. Si no se puede hacer en ese plazo se realizará posteriormente, acompañada de una explicación de motivos.

La notificación tendrá el contenido mínimo establecido en el artículo 33.3 del RGPD.

Se considera que existe constancia de una violación de la seguridad de los datos personales cuando hay certeza que esta se ha producido y se tiene un conocimiento suficiente de su naturaleza y su alcance.

Además, cuando sea probable que la violación comporte un alto riesgo para los derechos de las personas interesadas, el responsable tendrá que comunicarlo a estas sin más dilación indebida y en un lenguaje claro y sencillo.

3. Elección y vinculación con el encargado del tratamiento

Los responsables tienen que seleccionar encargados que ofrezcan garantías suficientes para aplicar las medidas técnicas y organizativas apropiadas, de forma que el tratamiento sea conforme al que se establece en el RGPD y en la Ley Orgánica 3/2018.

Así mismo, tienen que subscribir con ellos el contrato o acto jurídico que se prevé en el artículo 28 del RGPD.

b) ENCARGADOS

El RGPD establece una serie de obligaciones propias para los encargados del tratamiento:

a) Mantener un Registro de Actividades de Tratamiento (RAT).
b) Determinar las medidas de seguridad aplicables a los tratamientos que realizan.
c) Respetar el deber de confidencialidad.
d) Designar una persona delegada de protección de datos, en los casos en que así lo prevé el RGPD.
e) Posibilidad de adherirse a códigos de conducta o certificarse en el marco de los esquemas de certificación previstos en el mismo RGPD.
f) En caso de que subcontratan operaciones de tratamiento, hay que elegir subencargados que ofrezcan garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de forma que el tratamiento sea conforme a los requisitos del RGPD y la Ley Orgánica 3/2018.

10. CONCLUSIONES

Como conclusión a este trabajo, podemos confirmar que la normativa vigente de protección de datos personales tiene como principal objetivo salvaguardar la privacidad y los derechos fundamentales de las personas en lo que respecta al tratamiento de su información personal. Asimismo, las conclusiones más relevantes sobre esta normativa son las siguientes:

1. Protección Integral de Datos: el Reglamento General de Protección de Datos (RGPD) en la Unión Europea y la LODP en nuestro estado, establecen un marco sólido para la protección de datos personales, imponiendo obligaciones claras a las organizaciones que manejan dicha información. Estas obligaciones incluyen la necesidad de obtener el consentimiento explícito de los individuos para el procesamiento de sus datos, así como la implementación de medidas técnicas y organizativas adecuadas para garantizar la seguridad de los datos.

2. Derechos de los Titulares de los Datos: la normativa refuerza los derechos de los individuos sobre sus datos personales. Estos derechos incluyen el acceso a la información que se tiene sobre ellos, la rectificación de datos incorrectos, la eliminación de datos cuando ya no sean necesarios, y la portabilidad de datos, que permite a los individuos recibir sus datos en un formato estructurado y comúnmente utilizado.

3. Responsabilidad y Transparencia: las organizaciones deben demostrar conformidad con la normativa de protección de datos a través de la adopción de políticas de privacidad claras y transparentes, así como mediante la realización de evaluaciones de impacto de la privacidad y la designación de un responsable de protección de datos en ciertos casos. Esta responsabilidad proactiva contribuye a una mayor transparencia y confianza por parte de los usuarios.

4. Sanciones y Cumplimiento: la normativa incluye sanciones significativas para las organizaciones que no cumplan con las regulaciones de protección de datos. Estas sanciones pueden ser económicas y administrativas, y buscan incentivar el cumplimiento normativo. En el caso de las sanciones que se pueden imponer por el incumplimiento del RGPD, las multas pueden llegar hasta el 4% de la facturación anual global de una empresa, lo cual subraya la importancia de la conformidad.

5. Transferencia Internacional de Datos: la regulación establece estrictas condiciones para la transferencia de datos personales a terceros países o a organizaciones internacionales, asegurando que los niveles de protección de datos no se vean comprometidos. Esto se logra mediante mecanismos como las cláusulas contractuales estándar y las decisiones de adecuación emitidas por las autoridades de protección de datos.

6. Adopción Global y Adaptación Local: el RGPD ha sentado un precedente importante a nivel mundial, muchos países han adoptado y adaptado sus propias legislaciones de protección de datos basadas en principios similares; esto ha llevado a una mayor armonización global en cuanto a la protección de datos personales, aunque con variaciones que reflejan contextos y necesidades locales.

En resumen, la normativa vigente de protección de datos personales representa un avance significativo en la protección de la privacidad y los derechos de los individuos. A través de un marco legal robusto y detallado, se busca garantizar que los datos personales sean tratados de manera segura y transparente, promoviendo al mismo tiempo la confianza en el manejo de la información en una era digital.

11. PROPUESTA DE MEJORA

Para elaborar una propuesta de mejora sobre la normativa vigente sobre protección de datos, es esencial tener en cuenta las actuales regulaciones y los desafíos emergentes en el ámbito de la privacidad y la seguridad de la información.

La propuesta de mejora que presento sobre la normativa vigente de protección de datos se estructura como sigue a continuación e incluye recomendaciones específicas:

1- Introducción

La protección de datos personales es un derecho fundamental, y las normativas actuales, como el Reglamento General de Protección de Datos (RGPD) en la Unión Europea y la Ley de Protección de Datos Personales en varios países, han establecido un marco sólido y seguro de protección. No obstante, la rápida evolución tecnológica y la creciente digitalización requieren una actualización y mejora continua de estas normativas para abordar nuevos desafíos y fortalecer la protección de los datos personales.

2- Fortalecimiento de la Transparencia y el Consentimiento Informado

- Recomendación: mejorar los mecanismos de obtención de consentimiento, asegurando que sean claros, comprensibles y accesibles. Implementar formularios de consentimiento dinámicos que permitan a los usuarios entender fácilmente qué datos se recopilan, con qué propósito y cómo serán utilizados.

- Justificación: muchos usuarios aún no comprenden completamente cómo se utilizan sus datos. Formularios más claros y accesibles aumentarían la transparencia y mejorarían la confianza de las personas.

3- Inclusión de normativas para nuevas tecnologías

- Recomendación: ampliar la normativa para incluir directrices específicas sobre el uso de tecnologías emergentes como la inteligencia artificial, el internet de las cosas (IoT) y el big data. Establecer requisitos estrictos para la anonimización y la minimización de datos en estos contextos.

- Justificación: estas tecnologías presentan nuevos riesgos para la privacidad y requieren una regulación específica para garantizar que se manejen de manera segura y ética.

4- Fortalecimiento de la Seguridad de los Datos

- Recomendación: implementar requisitos más estrictos para la seguridad de los datos, incluyendo la obligatoriedad de utilizar cifrado avanzado y técnicas de seguridad de última generación. Además, se debe exigir la realización de auditorías periódicas de seguridad.

- Justificación: la seguridad de los datos es un componente crítico para la protección de la privacidad. Medidas de seguridad más estrictas y auditorías regulares ayudarán a prevenir brechas de datos y ciberataques.

5- Responsabilidad y sanciones más estrictas

- Recomendación: aumentar las sanciones para las empresas y organizaciones que no cumplan con las normativas de protección de datos. Establecer una escala progresiva de multas basadas en el nivel de negligencia y el daño causado.

- Justificación: las sanciones más estrictas actuarán como un disuasivo eficaz y asegurarán que las organizaciones tomen en serio sus responsabilidades en la protección de datos.

6- Mejora de los derechos de los titulares de los datos

- Recomendación: fortalecer los derechos de los titulares de los datos, incluyendo el derecho a la portabilidad de datos y el derecho al olvido. Facilitar mecanismos para que los individuos puedan ejercer estos derechos de manera sencilla y efectiva.

- Justificación: aumentar el control de los individuos sobre sus datos personales es fundamental para una protección de datos robusta. Derechos más fuertes y mecanismos accesibles empoderarán a los usuarios.

7- Educación y concienciación

- Recomendación: desarrollar programas de educación y concienciación sobre protección de datos dirigidos a ciudadanos, empresas y entidades gubernamentales. Estos programas deben incluir formación sobre mejores prácticas, riesgos asociados con el manejo de datos y los derechos de los individuos.

- Justificación: La educación y la concienciación son esenciales para fomentar una cultura de protección de datos y asegurar que todos los actores comprendan y respeten la normativa.

8- Conclusión

La mejora continua de la normativa de protección de datos es esencial para enfrentar los desafíos actuales y futuros. Las recomendaciones propuestas buscan fortalecer la transparencia, seguridad y responsabilidad en el manejo de datos personales, asegurando una protección más efectiva y adaptada a las nuevas realidades tecnológicas. Esta propuesta abarca aspectos clave para la mejora de la normativa vigente, buscando un equilibrio entre la innovación tecnológica y la protección efectiva de los derechos de los individuos.

NORMATIVA CONSULTADA

Constitución Española (BOE nº 311, de 29 de diciembre de 1978) < https://www.boe.es/eli/es/c/1978/12/27/(1)/con>

Carta de los Derechos Fundamentales de la Unión Europea <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:12012P/TXT >

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) <https://www.boe.es/doue/2016/119/L00001-00088.pdf>

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Vigente en los artículos referidos en la Disposición adicional decimocuarta y Disposición transitoria cuarta de la Ley Orgánica 3/2018, de 5 de diciembre. <https://www.boe.es/buscar/act.php?id=BOE-A-1999-23750>

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. <https://www.boe.es/buscar/pdf/2018/BOE-A-2018-16673-consolidado.pdf>

Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales. <https://www.boe.es/buscar/act.php?id=BOE-A-2021-8806>

Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. <https://www.boe.es/buscar/act.php?id=BOE-A-2008-979>

Real Decreto 389/2021, de 1 de junio, por el que se aprueba el Estatuto de la Agencia Española de Protección de Datos.< https://www.boe.es/buscar/act.php?id=BOE-A-2021-9175>

Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad. <https://www.boe.es/buscar/act.php?id=BOE-A-2022-7191>

DECRETO 195/2018, de 31 de octubre, del Consell, por el que aprueba el Reglamento orgánico y funcional de la Conselleria de Transparencia, Responsabilidad Social, Participación y Cooperación. [2018/10615] <https://dogv.gva.es/datos/2018/11/16/pdf/2018_10615.pdf>

Orden HFP/873/2021, de 29 de julio, por la que se aprueba la Política de Seguridad de la Información en el ámbito de la Administración digital del Ministerio de Hacienda y Función Pública.< https://www.boe.es/buscar/doc.php?id=BOE-A-2021-13777>

ORDEN 1/2021, de 20 de abril, de la consellera de Participación, Transparencia, Cooperación y Calidad Democrática, por la que se desarrolla el Decreto 179/2020, de 30 de octubre, del Consell, por el cual se aprueba el Reglamento orgánico y funcional de la Conselleria de Participación, Transparencia, Cooperación y Calidad Democrática. [2021/4126] (DOGV núm. 9069 de 26.04.2021) Ref. Base Datos 003697/2021 <https://dogv.gva.es/portal/ficha_disposicion_pc.jsp?sig=003697/2021&L=1>

BIBLIOGRAFÍA

Agencia Española de Protección de Datos | AEPD. (s. f.). https://www.aepd.es/

Almaida, C. A. (2007). *Estudio práctico sobre la protección de datos de carácter personal*. Lex Nova.

datos.gob.es. (2023, 27 abril). Una aproximación a los datos centrada en las personas. datos.gob.es. <https://datos.gob.es/es/blog/una-aproximacion-los-datos-centrada-en-las-personas>

Delegación de Protección de Datos de la Generalitat <https://presidencia.gva.es/es/web/delegacion-de-proteccion-de-datos-gva>

De la Fuente Miguélez, A. (2017). Aplicabilidad de la normativa sobre protección de datos de carácter personal en el ámbito de la función estadística pública. *Revista Vasca de Administración Pública. Herri-Arduralaritzako Euskal Aldizkaria*, (107), 275-301.

file:///C:/Users/pasta/Downloads/09_RVAP107-I_delaFuente-Miguelez%20DIG.pdf

Ejercicio del derecho de acceso, rectificación, supresión y portabilidad de sus datos personales, limitación y oposición del tratamiento y no ser objeto de decisiones individuales automatizadas respecto a sus datos personales registrados en la Generalitat. https://www.gva.es/es/inicio/procedimientos?id_proc=19970

Gómez, R. M. (2016). Contenido y novedades del Reglamento General de Protección de Datos de la UE (Reglamento UE 2016/679, de 27 de abril de 2016). *Gabilex: Revista del Gabinete Jurídico de Castilla-La Mancha*, (6), 243-280. <https://www.castillalamancha.es/sites/default/files/documentos/pdf/20160709/revista_gabilex_no_6._autor_roberto_mayor_gomez.pdf>

Guía de derechos de la ciudadanía en materia de protección de datos frente a la Generalitat https://gvaoberta.gva.es/documents/7843050/172663653/Gu%C3%ADa+de+derechos+de+la+ciudadan%C3%ADa+en+materia+de+protecci%C3%B3n+de+datos+frente+a+la+Generalitat/3bf6b5d2-901b-4eb5-8946-1246e2b74263

Guía sobre la aplicación del límite de la protección de datos en el derecho de acceso a la información pública https://presidencia.gva.es/documents/166475129/354927766/Gu%C3%ADa+protecci%C3%B3n+de+datos+-+transparencia.pdf/ffc2d917-6a74-0622-f460-f09b2e06f802?t=1679573019565

Janeiro, D. B., Pérez, A. P., Tesón, I. V., Hermosa, P. I. B., Sanz, M. F. M., Llombart, P. A., & Cariñana, M. Á. Z. (2021). *Nuevas tecnologías y responsabilidad civil*. Editorial Reus.

LABORA https://labora.gva.es/documents/166000883/169069246/Informaci%C3%B3n+adicional+protecci%C3%B3n+de+datos.pdf/bf8c6aca-7964-4ae9-bd50-4c2848f90263

La protección de datos personales 'post mortem'. (s. f.). revistas.eleconomista.es. <https://revistas.eleconomista.es/buen-gobierno/2021/septiembre/la-proteccion-de-datos-personales-post-mortem-IF8986129>

Marina. (2024, 14 mayo). Datos personales: definición, tipos y ejemplos. Grupo Atico34. <https://protecciondatos-lopd.com/empresas/datos-personales>

Masciotra, M., EL, I. B. T. P., & DATA, H. (2004). La voz y la imagen y el ámbito de aplicación de la ley de protección de datos personales. *Dossier: Habeas Data*, 442.

<http://www.saij.gob.ar/mario-masciotra-voz-imagen-ambito-aplicacion-ley-proteccion-datos-personales-dacf040044-2004-04-28/123456789-0abc-defg4400-40fcanirtcod>

<https://jurisbibliotecadigital.com/administracion/frm-libros/pdf/1696600261_habeas_data.pdf#page=443>

Rallo Lombarte, A. (2019). *El nuevo derecho de protección de datos*. <https://repositori.uji.es/xmlui/bitstream/handle/10234/189958/rallo_2019_Eln.pdf?sequence=1&isAllowed=y>

Zaballos Pulido, E. (2013). *La protección de datos personales en España: evolución normativa y criterios de aplicación.* <https://docta.ucm.es/rest/api/core/bitstreams/3f978580-ba99-4606-a0c0-4be1ab41e626/content>

ANEXO I. RELACIÓN DEL TRABAJO CON LOS OBJETIVOS DE DESARROLLO SOSTENIBLE DE LA AGENDA 2030

Anexo al Trabajo de Fin de Grado y Trabajo de Fin de Máster: Relación del trabajo con los Objetivos de Desarrollo Sostenible de la agenda 2030.

Grado de relación del trabajo con los Objetivos de Desarrollo Sostenible (ODS).

Objetivos de Desarrollo Sostenibles	Alto	Medio	Bajo	No Procede
ODS 1. **Fin de la pobreza.**				
ODS 2. **Hambre cero.**				
ODS 3. **Salud y bienestar.**				
ODS 4. **Educación de calidad.**				
ODS 5. **Igualdad de género.**				
ODS 6. **Agua limpia y saneamiento.**				
ODS 7. **Energía asequible y no contaminante.**				
ODS 8. **Trabajo decente y crecimiento económico.**				
ODS 9. **Industria, innovación e infraestructuras.**	x			
ODS 10. **Reducción de las desigualdades**.		x		
ODS 11. **Ciudades y comunidades sostenibles**.				
ODS 12. **Producción y consumo responsables.**				
ODS 13. **Acción por el clima.**				
ODS 14. **Vida submarina.**				
ODS 15. **Vida de ecosistemas terrestres.**				
ODS 16. **Paz, justicia e instituciones sólidas.**	x			
ODS 17. **Alianzas para lograr objetivos.**	x			

Descripción de la alineación del TFG/TFM con los ODS con un grado de relación más alto.

***Utilice tantas páginas como sea necesario.

Editor: Secretaria General / UPV · D.L.: V-5092-2006 · ISSN: 1887-2298 · www.upv.es/secgen

Anexo al Trabajo de Fin de Grado y Trabajo de Fin de Máster: Relación del trabajo con los Objetivos de Desarrollo Sostenible de la agenda 2030. (Numere la página)

La relación de este Trabajo de Fin de Grado (TFG) con los Objetivos de Desarrollo Sostenible (ODS) se concreta en los objetivos 9, 10, 16 y 17.

Objetivo 9: Industria, Innovación e Infraestructura
El ODS 9 hace referencia a la construcción de infraestructuras resilientes, la promoción de la industrialización inclusiva y sostenible, y el fomento de la innovación. Este TFG se relaciona con este objetivo a través de la promoción de condiciones legales adecuadas en el ámbito del tratamiento de datos, lo cual fomenta el desarrollo de infraestructuras digitales sólidas que garantizan los derechos de privacidad. Al asegurar que la infraestructura tecnológica respeta y protege los datos personales, se impulsa un entorno de innovación seguro y confiable.

Objetivo 10: Reducción de las Desigualdades
El ODS 10 se centra en reducir la desigualdad dentro de los países y entre ellos. En el contexto del tratamiento de datos, este objetivo se vincula con la implementación de condiciones legales claras y equitativas. Un marco legal robusto garantiza que todos los individuos, independientemente de su origen o posición social, tengan igualdad de derechos en cuanto a la privacidad y protección de sus datos. Este TFG contribuye a este objetivo al proponer prácticas legales que aseguren la equidad en la protección de datos para todos.

Objetivo 16: Paz, Justicia e Instituciones Sólidas
El ODS 16 promueve sociedades pacíficas e inclusivas, el acceso a la justicia para todos y la creación de instituciones eficaces, responsables e inclusivas a todos los niveles. La protección de datos personales es esencial para este objetivo, ya que garantiza la privacidad y seguridad de los individuos, aspectos clave para construir sociedades justas y pacíficas. Este TFG aborda la necesidad de establecer condiciones legales sólidas en el tratamiento de datos, contribuyendo así a la promoción de la paz y la justicia.

Objetivo 17: Alianzas para Lograr los Objetivos
El ODS 17 enfatiza la necesidad de revitalizar la alianza mundial para el desarrollo sostenible. En el ámbito del tratamiento de datos personales, la consecución de este objetivo requiere la colaboración y alianzas entre diferentes actores, como gobiernos, empresas y la sociedad civil. Establecer condiciones legales efectivas fomenta estas alianzas y contribuye a la gestión ética de la información personal. Este TFG promueve la creación de marcos colaborativos que faciliten la protección de datos a través de esfuerzos conjuntos.

En conjunto, este TFG contribuye a avanzar hacia un entorno más justo, equitativo, innovador y colaborativo. Al alinearse con varios ODS, se promueven prácticas éticas en el tratamiento de datos personales, lo que es esencial para el desarrollo sostenible y la creación de sociedades inclusivas y pacíficas.

Editor: Secretaria General / UPV · D.L.: V-5092-2006 · ISSN: 1887-2298 · www.upv.es/secgen