Estudio sobre el sistema de protección de datos personales con finalidad de prevención, detección e investigación policial de infracciones penales

Coordinador: Carlos Manuel Fernández González

Autores: David Teatino Gómez, Carlos Manuel Fernández González, Juan José Hernández Domínguez, Alba Arqueros Tornos y Jesús Javier Camacho Fernández

GOBIERNO DE ESPAÑA
MINISTERIO DEL INTERIOR

Estudio sobre el sistema de protección de datos personales con finalidad de prevención, detección e investigación policial de infracciones penales

Coordinador:
Carlos Manuel Fernández González

Autores:
David Teatino Gómez, Carlos Manuel Fernández González, Juan José Hernández Domínguez, Alba Arqueros Tornos, Jesús Javier Camacho Fernández

Madrid, 2022

Catálogo de Publicaciones de la Administración General del Estado:
https://cpage.mpr.gob.es

Información del Ministerio del Interior:

Teléfono: 060
Internet: www.interior.gob.es

Edita:

MINISTERIO DEL INTERIOR
SECRETARÍA GENERAL TÉCNICA

Fecha de edición: Junio 2022
NIPO (ed. papel): 126-22-008-6
NIPO (en línea): 126-22-009-1
ISBN: 978-84-8150-335-7
Depósito Legal: M-11352-2022

Maquetación e impresión: DiScript Preimpresión, S. L.
Calle del Hierro, 33, 28045 Madrid

Índice

PRÓLOGO

En una sociedad digitalizada y tecnificada como la actual, la información y el mensaje o los datos que contiene, cobran una relevancia nunca vista en la Historia de la humanidad. El volumen de datos tratados y almacenados, la capacidad de su análisis, el periodo durante el que pueden ser conservados y la extensión de estas actuaciones a lo largo y ancho del planeta, ha alcanzado niveles difícilmente imaginables hace solamente una década.

Esta cuestión reviste especial importancia cuando se tratan datos capaces de identificar a una persona física y, con ello, poder atribuirla innumerables cualidades o rasgos (lugar de residencia, opiniones, religión, opciones sexuales, etc.). Esta información singular es lo que se puede definir como «datos personales» o «datos de carácter personal».

Dichas magnitudes, que pueden ser esenciales para el desarrollo de la personalidad y del disfrute de los derechos fundamentales que nos asisten, al poder ser atribuidas directamente a una persona, se convierten en atributos inherentes al individuo que pueden ser conocidos y utilizados por terceros con distintos objetivos o finalidades.

La facultad que nos asiste para que estas actuaciones sobre nuestros datos personales se produzcan respetando los Derechos Humanos y conforme a la legalidad vigente, así como la definición o extensión de este derecho, tendrá una acepción y unas garantías diferentes en virtud de la parte del mundo donde se pretenda ejercer.

En el caso de las sociedades democráticas como la española y las del resto de los Estados Miembros de la Unión Europea, el derecho a la protección de datos personales se ha convertido en Derecho Fundamental incorporado en varios de nuestros textos legales básicos (la Carta de los Derechos Fundamentales, el Tratado de Funcionamiento de la Unión y nuestra propia Constitución), por lo que, al igual que el resto de estos Derechos, queda enmarcado en la esencia propia de nuestras libertades y debe ser garantizado y protegido de conformidad con dicho estatus.

Aunque esta preocupación por proteger la información o las cuestiones íntimas relativas a las personas podemos encontrarla a lo largo del desarrollo de las civilizaciones, el significado y el contenido del mismo han sufrido numerosos cambios para adaptarse al modelo de sociedad en donde debía desplegar sus efectos.

En la Grecia clásica, primera sociedad en escribir libros y poemas siete siglos a.d.C., ya se recogía entre los mensajes de sus mitos la importancia de no conocer

las cuestiones sobre terceros sin necesidad. Prometeo, a diferencia de lo que se cree popularmente, no fue castigado únicamente por darle el fuego al hombre, sino que la causa que finalmente le condenó, fue intentar evitar que el plan de Zeus urdido para que Pandora abriera la caja privada que éste le había dado a su prometido fracasara (cosa que sabemos que no consiguió).

El concepto moderno de protección de datos o «privacidad», suele ser atribuido al contenido del famoso artículo *«The right of privacy»* publicado en «*Harvard Law Review*» por Warren y Brandeis el 15 de diciembre de 1890.

Estos autores, entre otras cuestiones, entendían que la intensidad y la complejidad de la vida ya a finales del Siglo XIX, hacía necesario implementar el concepto «*The right to be alone»,* como el derecho a cierta retirada del mundo y de la influencia de la nueva cultura de esa sociedad, de modo que la privacidad se volvía más esencial, si cabía, para las personas.

Un famoso ejemplo acaecido cinco años después, derivó de la publicación el 20 de abril de 1895 en el periódico «*The illustrated Police News (Law Courts and Weekly Rercod)»*, donde se exhibía caricaturizado a Oscar Wilde a su llegada a los Juzgados abucheado por la turba y enfermo en prisión por haber sido juzgado únicamente por su orientación sexual. Esto tuvo una repercusión que fue desmedida para una figura como la de este escritor universal.

En este más de un siglo recorrido, la situación del bloque de la protección de datos personales ha avanzado, quizás no lo que nos gustaría, pero se va consolidando como un elemento básico de nuestra convivencia, la defensa de los derechos, la igualdad, la libertad, la seguridad y como herramienta contra la discriminación, los prejuicios y la prevención de los delitos de odio.

La Unión Europea y los Estados Miembros, a partir de varios instrumentos promulgados en el año 2016, han implantado un sistema dividido principalmente en tres grandes bloques: el general, el de las propias instituciones de la Unión y el específico para el tratamiento de datos con fines de prevención, detección, investigación y enjuiciamiento de delitos, así como para la ejecución de las penas.

Si con carácter general proteger este derecho fundamental resulta una cuestión primordial, en el campo «*policial*» es ineludible establecer un marco sólido y coherente que cuente con el respaldo de una ejecución estricta por parte de las Autoridades competentes. Esto, sin que sea óbice para que éstas cumplan con sus misiones y sea facilitada la libre circulación de datos personales entre las mismas con los fines aludidos.

Para que esto se produzca, una de las principales obligaciones de los responsables es promover la formación y la concienciación de todas las personas que pertenecen a sus organizaciones, especialmente, en el caso de los cuerpos policiales.

La Secretaría de Estado de Seguridad, en el marco del Real Decreto 734/2020, de 4 de agosto, por el que se desarrolla la estructura orgánica básica del Ministerio del Interior, a través de la Dirección General de Coordinación y Estudios, es el órgano competente para desarrollar acciones formativas comunes para las miembros de las Fuerzas y Cuerpos de Seguridad.

Por ese motivo, su personal desarrolla este tipo de estudios con la idea de que la formación sea una herramienta fundamental para lograr que policías y guardias civiles esten adaptados lo mejor posible las necesidades de una «*sociedad del*

dato». Cuestión esta que abarcaría tanto la formación inicial como la de perfeccionamiento en esta materia.

El objetivo es que los trabajos y su contenido vayan dirigidos a todos los miembros de las organizaciones y a todas las personas interesadas o implicadas, seleccionando escrupulosamente el contenido de los materiales y temarios.

Contar con personal especializado formado en esta materia garantiza una atención especializada a las demandas que requiere la sociedad en cada momento, con la dificultad añadida de la rápida evolución tecnológica y fáctica que, en la mayoría de las veces, adelanta al legislador, lo que exige un esfuerzo mayor si cabe, en la aplicación de las normas.

Decía el propio Oscar Wilde que *«No existen más que dos reglas para escribir: tener algo que decir y decirlo.»*

Los autores de este estudio, que son profesionales pioneros en esta materia y que tratan estas cuestiones diariamente, han compendiado los aspectos más relevantes de la legislación especial en materia policial, de manera que el material resultante se convierte en un instrumento útil de estudio y consulta, no solo para las Fuerzas y Cuerpos de Seguridad, sino para toda aquella persona que deba tratar datos en este campo.

De hecho, entiendo que el *«Estudio sobre el sistema de protección de datos personales con la finalidad de prevención, detección e investigación policial de infracciones penales»* es un libro que debería ser de lectura aconsejada para cualquiera que pretenda iniciarse en la materia.

Rafael Pérez Ruiz
Secretario de Estado de Seguridad

CAPÍTULO 1
CONCEPTOS GENERALES

I. ANTECEDENTES Y SITUACIÓN (BLOQUES NORMATIVOS BÁSICOS EN ESTE ÁMBITO)

1. Antecedentes

Dada la trascendencia sobre los derechos fundamentales de las personas, es indiscutible la importancia del tratamiento de los datos de carácter personal en la sociedad actual, donde el desarrollo de la tecnología y de los medios o sistemas de comunicación nos permiten afirmar que vivimos en una realidad 3.0. De hecho, la creciente digitalización es definida por algunos especialistas con el sentido de que *«Digitalizar implica crear un registro, poner etiquetas a las cosas para que sea más fácil encontrarlas y seguirlas. Digitalizar equivale a hacer rastreable aquello que no lo era.»,* de modo que entienden que ese rastreo no es sino una forma de vigilar a los interesados con distintos objetivos[1].

Esta circunstancia cobra especial relevancia cuando los fines de las actuaciones a llevar a cabo con los datos que identifican a las personas, tanto de forma digital como analógica, van dirigidas a la prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de las penas.

Siendo esto de enorme relevancia, sobre todo cuando hablamos de datos de personas que han resultado víctimas o perjudicadas por las conductas delictivas.

Todo esto porque no se puede hablar de garantizar la seguridad de las personas y la protección de sus derechos sin el tratamiento de sus datos personales y sin implementar sistemas jurídicos que los protejan. La necesidad de identificar a las personas autoras de los delitos, proteger a las víctimas, prevenir la comisión de ilícitos como los de violencia de género, la cibercriminalidad (basada o no en procedimientos de ingeniería social), obtener información esencial para la seguridad ciudadana y un largo número de misiones atribuidas los organismos correspondientes, no sería posible sin las actividades de tratamiento que permitieran a dichas autoridades cumplir con sus cometidos.

---

[1] VÉLIZ, C. «*Digitalizar es vigilar*» Tribuna. Diario el País. 03 dic 2021 https://elpais.com/opinion/2021-12-03/digitalizar-es-vigilar.html

Se comparte la valoración de buena parte de la doctrina científica al entender que la protección de datos de carácter personal en este marco, sería como la «*venda que cubre los ojos a la Justicia*», una condición indispensable para que las Autoridades competentes ejerzan sus funciones con absoluto respeto a la Constitución y al resto del ordenamiento jurídico, actúen durante el cumplimiento de sus misiones con absoluta neutralidad política e imparcialidad y, en consecuencia, sin sesgos de discriminación alguna por razón de raza, religión u opinión y con el objetivo de mantener la aplicación del Derecho penal del Hecho, en contraposición al Derecho Penal de Autor.

Aunque no es la base de los derechos ni era el primer instrumento aplicable, el Reglamento General de Protección de Datos[2] ha supuesto un hito en el marco legal de la protección de datos de la Unión Europea.

Este Reglamento, al que los expertos atribuyen «*alma de Directiva*» por la posibilidad de adaptación y desarrollo por los Estados miembros, pretende tener alcance general y tiene por objeto, por un lado, el fijar las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y, por el otro, de mucha importancia *(aunque generalmente suele obviarse al analizarlo)*, el facilitar su libre circulación en la propia Unión.

Junto con el RGPD, derivado principalmente de los instrumentos previstos en el Plan de Acción del Programa de Estocolmo, la UE ha dictado una serie de instrumentos que a nuestro juicio son de obligado conocimiento por parte de las personas que tendrán que operar con datos de carácter personal en el ámbito policial. Aunque se pormenorizarán posteriormente con detalle, procedemos a enumerar los más relevantes en este punto:

- 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 y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.[3]
- Directiva (UE) 2016/681 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la utilización de datos del registro de nombres de los pasajeros (PNR) para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave.
- Directiva (UE) 2019/1153 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, por la que se establecen normas destinadas a facilitar el uso de información financiera y de otro tipo para la prevención, detección, investigación o enjuiciamiento de infracciones penales y por la que se deroga la Decisión 2000/642/JAI del Consejo.

[2] 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://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX%3A32016R0679

[3] https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX%3A32016L0680

- Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión de enfoque transversal a las tres anteriores.
- Directiva (UE) 2019/770 del Parlamento Europeo y del Consejo, de 20 de mayo de 2019, relativa a determinados aspectos de los contratos de suministro de contenidos y servicios digitales (Texto pertinente a efectos del EEE.)
- Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas). Cuyo contenido se prevé sea sustituido por el futuro Reglamento ePrivacy[4].
- Reglamento (UE) 2016/794 del Parlamento Europeo y del Consejo, de 11 de mayo de 2016, relativo a la Agencia de la Unión Europea para la Cooperación Policial (Europol). Capítulo VI (sobre las garantías de protección de datos)
- Reglamento (UE) 2017/1939 del Consejo, de 12 de octubre de 2017, por el que se establece una cooperación reforzada para la creación de la Fiscalía Europea. Capítulo VIII (sobre protección de datos)
- Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) n.o 45/2001 y la Decisión n.o 1247/2002/CE (Reglamento Instituciones UE)
- Reglamento (UE) 2019/818 del Parlamento Europeo y del Consejo, de 20 de mayo de 2019, relativo al establecimiento de un marco para la interoperabilidad entre los sistemas de información de la UE en el ámbito de la cooperación policial y judicial, el asilo y la migración y por el que se modifican los Reglamentos (UE) 2018/1726, (UE) 2018/1862 y (UE) 2019/816.
- Reglamento (UE) 2019/817 del Parlamento Europeo y del Consejo, de 20 de mayo de 2019, relativo al establecimiento de un marco para la interoperabilidad de los sistemas de información de la UE en el ámbito de las fronteras y los visados y por el que se modifican los Reglamentos (CE) n.° 767/2008, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 y (UE) 2018/1861 del Parlamento Europeo y del Consejo, y las Decisiones 2004/512/CE y 2008/633/JAI del Consejo
- Directiva (UE) 2019/1024 del Parlamento Europeo y del Consejo de 20 de junio de 2019 relativa a los datos abiertos y la reutilización de la información del sector público.
- Reglamento (UE) 2018/1807 del Parlamento Europeo y del Consejo, de 14 de noviembre de 2018, relativo a un marco para la libre circulación de datos no personales en la Unión Europea (Texto pertinente a efectos del EEE.)

[4] Para más información ver: Declaración relativa al Reglamento sobre la privacidad y las comunicaciones electrónicas y el papel futuro de la Autoridad de control y el CEPD Adoptada el 19 de noviembre de2020 https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_20201119_eprivacy_regulation_es.pdf

No podemos obviar tampoco otros sistemas basados en tratamiento de datos personales como el Servicio Europeo de Información de Antecedentes Penales (*ECRIS por sus siglas en inglés European Criminal Records Information Services*) que desarrolla una base de datos centralizada con información sobre condenas de nacionales de terceros países y personas apátridas (ECRIS-TCN), el Sistema Europeo de Indice de Ficheros Policiales (*EPRIS por sus siglas en inglés European Police Records Information System)* que se encuentra en una fase embrionaria de desarrollo y el Acuerdo entre la Unión Europea y los Estados Unidos de América relativo al tratamiento y la transferencia de datos de mensajería financiera de la Unión Europea a los Estados Unidos a efectos del Programa de seguimiento de la financiación del terrorismo[5].

Y por supuesto, habrá que seguir muy de cerca la tramitación la propuesta de Reglamento sobre inteligencia artificial que la Comisión Europea hizo pública el 21 de abril de 2021[6], la cual tendrá un influencia directa en este framework cuando se realicen labores de uso de datos biométricos a distancia, descripción de los sistemas I.A., perfilados automáticos, etc., y el desarrollo de los instrumentos de la Unión Europea sobre Servicios Digitales (Digital Services Act- DSA) y de Mercados Digitales (Digital Markets Act-DMA) y la futura Ley del Dato (Data Act)[7] de la Unión, que esperemos entren en vigor próximamente.

Los instrumentos apuntados están reseñados sin ánimo de exhaustividad puesto que es tanta la importancia de la protección de datos y las relaciones electrónicas, que existen otras muchas normas y proyectos que afectan y afectarán en la materia tanto a nivel internacional como interno. Vid. e.j. el proyecto de Reglamento del Parlamento Europeo y del Consejo sobre la lucha contra la difusión de contenidos terroristas en línea o a la Directiva (UE) 2019/1937, de 23 de octubre de 2019, relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión (Directiva alertadores o whistleblowers)

Todas las normas y sistemas señalados tratan y se basan en una concepción que se emplea mucho -*los datos personales*- pero cuyo significado, concepto y extensión no está tan claro que sea conocido por la mayoría de los actores que los manejan ni por los propietarios de dichos datos: *los interesados.*

Esta cuestión comenzaría con determinar y ser conscientes del contenido y la extensión del derecho fundamental a la protección de datos de carácter personal y su diferencia con otros derechos fundamentales cuyos elementos son parecidos y complementarios pero que no dejan de ser diferentes en muchos factores como por ejemplo los derechos a la intimidad, al honor o a la propia imagen.

El concepto o alusión a lo íntimo y lo privado lo podemos encontrar desde antiguo en textos como el Juramento Hipocrático: «*Todo lo que vea y oiga en el ejercicio de mi profesión, y todo lo que supiere acerca de la vida de alguien, si es cosa que no debe ser divulgada, lo callaré y lo guardaré con secreto inviolable.*», la

[5] https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A22010A0727%2801%29

[6] https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonisedrules-artificial-intelligence-artificial-intelligence

[7] COM (2022) 68: Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), consultada en la web: https://eur-lex.europa.eu/procedure/EN/2022_47

Biblia: «*Mateo 6:5-6 Y cuando oréis, no seáis como los hipócritas; porque a ellos les gusta ponerse en pie y orar en las sinagogas y en las esquinas de las calles, para ser vistos por los hombres. En verdad os digo {que ya} han recibido su recompensa. Pero tú, cuando ores, entra en tu aposento, y cuando hayas cerrado la puerta, ora a tu Padre que está en secreto, y tu Padre, que ve en lo secreto, te recompensará.*», el Corán: «*¡Invocad a vuestro Señor humilde y secretamente! El no ama a quienes violan la ley. (Corán, 7:55)*» o el Código de Hammurabi: «*Si este esclavo no ha querido mencionar el nombre de su dueño, le llevará al palacio; (allí) se realizará una investigación y se lo devolverán a su dueño.*»

En cuanto al tema concreto de datos personales, la obligación de facilitar y tratar datos de las personas por parte de las distintas autoridades civiles y/o eclesiásticas ha sido un constante a lo largo de nuestra historia. Se pueden citar un sinfín de ellas, pero es clarificadora la *«Real orden disponiendo se recuerde a los particulares, entidades, Autoridades y funcionarios la obligación de facilitar a la Administración provincial los datos que ésta pida para la exacción del impuesto de cédulas personales»*[8] que concluía con: *«...(...)... S. M. el Rey (q. D. g :) se ha servido resolver que, con carácter general, se recuerde a los particulares o entidades, Autoridades y funcionarios la obligación en que se encuentran de facilitar a la Administración provincial los datos que ésta les pida para la exacción del impuesto de cédulas personales, bajo apercibimiento de incurrir en las sanciones a que dicho artículo se refiere y que serán inexorablemente exigidas.»*

Más allá del significado de estas nociones, el desarrollo de sistemas legales de protección de cada uno de los derechos que soportan éstas iría de la mano del devenir de los siglos XIX y XX donde el desarrollo técnico jurídico y las declaraciones de derechos vendrían a consolidarlos cada uno con su contenido formal y material.

En este momento, las corrientes doctrinales distinguen básicamente cuatro o cinco tipos o generaciones de derechos humanos:

- En la primera se encajan las libertades individuales frente a la injerencia de los poderes públicos, requiriendo sus límites y tutelándose por la observancia derechos de tipo individual (derecho a la vida, la integridad física y mental, libertad, seguridad, etc.)
- En la segunda, se encontrarían los derechos laborales, económicos, sociales y culturales, los cuales exigen una política activa para garantizar su ejercicio.
- En la tercera generación, entre los que se encuentran la autodeterminación de la personalidad, la paz, la justicia internacional, el medio ambiente, patrimonio o las condiciones de vida digna, se incluiría la libertad informática como un nuevo derecho del individuo a tutelar su propia identidad informática, concretándose en las garantías de acceso y control de las informaciones procesadas en ficheros de datos por parte de las personas interesadas.

  Es en este instante donde van a surgir las denominadas generaciones de leyes de protección de datos personales.

[8] https://www.boe.es/datos/pdfs/BOE//1926/117/A00548-00548.pdf

- En la cuarta generación, los derechos se refieren al desarrollo de actuaciones de las personas en el espacio digital. Entre estos nos encontramos la mayoría de los que se contienen en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, entre los que tenemos el derecho de acceso a la informática, a acceder al espacio de la sociedad de la información en condiciones de igualdad y de no discriminación, al uso del espectro digital, a la neutralidad de la red, a la seguridad digital, al control de la Inteligencia Artificial, educación digital, derecho al olvido, derecho a la desconexión en el ámbito laboral, teletrabajo, etc.

Incluso se estudian en la actualidad derechos de quinta generación cuyo exponente principal serían los neuro-derechos o «*derechos del cerebro*» concepto que se puede entender en dos aspectos: la privacidad mental, es decir, que por ejemplo los datos del cerebro de las personas se traten con una confidencialidad equiparable a la de los de los trasplantes de órganos. Y el segundo, el derecho a la identidad, manteniendo la individualidad de las personas[9].

Las corrientes doctrinales más avanzadas, entienden que éstos consistirían en cinco nuevos derechos humanos:

- Derecho a la privacidad mental (los datos cerebrales de las personas)
- Derecho a la identidad y autonomía personal
- Derecho al libre albedrío y a la autodeterminación
- Derecho al acceso equitativo a la aumentación cognitiva (para evitar producir inequidades)
- Derecho a la protección de sesgos de algoritmos o procesos automatizados de toma de decisiones.

Como referencia a nivel mundial en este campo, nuestro país, España, ha publicado la Carta de Derechos Digitales[10]que, aun no siendo un instrumento normativo y sin crear nuevos derechos, trata de perfilar los límites de los derechos más relevantes en el entorno y los espacios digitales y describir derechos instrumentales o auxiliares de los primeros.

Del mismo modo, la Comisión Europea ha presentado una propuesta de Declaración de Principios y Derechos Digitales de la Unión[11] *(European Declarationon Digital Rights and Principles for the Digital Decade, COM (2022) 28 final),* que pretende que sea aprobada al máximo nivel antes del verano del 2022, cuyo objetivo sería asegurar los valores, derechos y libertades garantizados por su legislación y que éstos salgan reforzados tanto en el entorno digital como fuera del mismo.

Esta Declaración se conforma en seis grandes bloques o capítulos que ponen claramente de manifiesto las intenciones de la Comisión: I. Poner a las personas

[9] YUSTE, Rafael. (2019). Disponible en: http://derecho.uc.cl/es/noticias/23763-neurocientifico-rafael-yuste-plantea-proteger-los-derechos-de-la-mente

[10] https://www.lamoncloa.gob.es/presidente/actividades/Documents/2021/140721-Carta_Derechos_Digitales_RedEs.pdf

[11] https://digital-strategy.ec.europa.eu/en/library/declaration-european-digital-rights-and-principles

en el centro de la transformación digital; II. Solidaridad e inclusión; III. Libertad de elección; IV. Participación en el espacio público digital; V y VI. Sostenibilidad.

Dentro del punto V «*Seguridad, protección y empoderamiento*», refuerza las ideas por las que: *«Toda persona tiene derecho a la protección de sus datos personales en línea. Este derecho incluye el control sobre cómo se utilizan los datos y con quién se comparten. Toda persona tiene derecho a la confidencialidad de sus comunicaciones y de la información contenida en sus dispositivos electrónicos, y nadie podrá ser sometido a medidas ilegales de vigilancia o a medidas de interceptación. Toda persona debe poder determinar su legado digital, y decidir qué pasa con la información disponible públicamente que le concierne, después de su muerte.»*

Por ello se expresa el compromiso de: *«Garantizar la posibilidad de trasladar fácilmente los datos personales entre diferentes servicios digitales».*

Entre estos «*nuevos* derechos» nos encontraríamos con Derechos ante la inteligencia artificial, los Derechos digitales en el empleo de las neurotecnologías, el Derecho al pseudonimato, el Derecho a la herencia digital y un largo etc.

Sin dejar de remarcar el profundo cambio que, para su ejercicio, pueda derivarse cuando se desarrollen los sistemas de realidad virtual aumentada, como el anunciado «*metaverso*»[12] o el desarrollo de todos los componentes de lo que denominamos la «*Web3*», lo que nos obligará probablemente a desarrollar nuevos derechos de «*metaseguridad*» o «*derechos enfocados en sistemas descentralizados o de registro distribuido*» donde los interesados controlen mucho más su información y los datos, cediendo los mínimos posibles.

Siendo un ejemplo de estas amenazas es que ya existen medios que se han hecho eco de las primeras denuncias por acoso, pederastia y agresión sexual en un metaverso,[13] lo cual nos facilita una muestra de las distintas problemáticas que estarían por venir.

En orden a fijar el iter temporal de la evolución de este derecho, en las sociedades democráticas, la mayor parte de los expertos[14] entienden como germen de la composición del derecho a la protección de datos el artículo *«The Right to Privacy»* que Samuel D. Warren y Louis D. Brandeis, publicaron en la revista *«The Harvard Law Review»* (volumen. IV, 15-XII-1890)[15] Entendiéndose esta *«privacy»* como el derecho a no ser molestado *«the right to be let alone»* en una época en el que el desarrollo de nuevas tecnologías (fotografía, teléfono, etc.) y los entonces medios de comunicación de masas (diarios, magazines, etc.) hacían cada vez más fácil atentar contra el espacio íntimo y privado de las personas y difundir estas vulneraciones a un número mayor de personas.

---

[12] https://www.businessinsider.es/metaverso-sera-desafio-privacidad-pero-europa-tiene-armas-978483

[13] https://tecnolawyer.com/es/la-agresion-sexual-ya-esta-pasando-al-metaverso/ y https://www.theverge.com/2021/12/9/22825139/meta-horizon-worlds-access-open-metaverse

[14] Vid. WARREN, S. D. y BRANDEIS, L. D. (1995). El derecho a la intimidad, edición a cargo de Benigno Pendás y Pilar Baselga, Madrid, Civitas, pág. 17. Para la revisión de la edición, vid. los comentarios de ARCE JANARIZ, A. (1996). Revista Española de Derecho Constitucional, núm. 47, págs. 367-371; y de GARCÍA ROCA, J. (1996). Revista de las Cortes Generales, núm. 37, págs. 473-483.

[15] https://dej.rae.es/lema/privacidad

Posteriormente, derivado de las prácticas de algunos Estados[16] y, sobre todo, tras el horror de la Segunda Guerra Mundial[17] y después de varias vicisitudes cuyo análisis excedería con mucho el contenido de esta obra, este derecho tuvo su reflejo en la Declaración Universal de los Derechos Humanos de 10 de diciembre de 1948, cuando disponía en su artículo 12 que:

> *«Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.»*

En nuestro ámbito de derecho comparado y social, el Convenio para la Protección de los Derechos Fundamentales y de las Libertades Públicas (CEDH) firmado en Roma el 4 de noviembre de 1950[18], recoge en su artículo 8 que:

> *«1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia. 2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás»*

El Pacto Internacional de Derechos Civiles y Políticos, de 16 de diciembre de 1966 (ICCPR) incidió de nuevo en esta cuestión y dispuso en su artículo 17 que toda persona tiene derecho *«a la privacidad y su protección por la ley.»*

El Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, hecho en Estrasburgo el 28 de enero de 1981 (Convenio 108)[19] marca un hito al tratar específicamente sobre el derecho a la protección de datos definiendo su objeto y fin como:

---

[16] En la década de los años 20, en Estados de los Estados Unidos de América como Virginia, se etiquetaba a las personas en relación con su raza y color de piel y se les prohibía casarse con personas etiquetadas de manera diferente, se les segregaba en los colegios, etc.

[17] HERNÁNDEZ VELASCO. I. *«Carissa Véliz, profesora de Oxford: "La falta de privacidad ha causado, indirectamente, más muertes que el terrorismo"15 octubre 2020. Durante la Segunda Guerra Mundial, por ejemplo, los nazis visitaban los registros públicos para buscar a los judíos. En Francia, en donde el censo no recababa información sobre religión por razones de privacidad, sólo encontraron y mataron al 25% de la población judía. En Holanda, en donde existían registros muy detallados sobre domicilio y religión, encontraron y asesinaron en torno al 75% de la población judía. La diferencia es de cientos de miles de personas.* https://www.bbc.com/mundo/noticias-54476232»

[18] Vid. Resolución de 5 de abril de 1999, de la Secretaría General Técnica, por la que se hacen públicos los textos refundidos del Convenio para la protección de los derechos y de las libertades fundamentales, hecho en Roma el 4 de noviembre de 1950; el protocolo adicional al Convenio, hecho en París el 20 de marzo de 1952, y el protocolo número 6, relativo a la abolición de la pena de muerte, hecho en Estrasburgo el 28 de abril de 1983. https://www.boe.es/buscar/act.php?id=BOE-A-1999-10148

[19] https://www.boe.es/buscar/doc.php?id=BOE-A-1985-23447

> *«...(...)...garantizar, en el territorio de cada Parte, a cualquier persona física sean cuales fueren su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona ("protección de datos")»*

Con el Protocolo que ha modificado este Convenio 108 (ahora denominado Convenio 108 +) se pretende extender su ámbito de aplicación, aumentar el nivel de protección de los datos personales y mejorar su eficacia en cuanto a los resultados a garantizar[20]. Este instrumento se ha convertido en el primer instrumento internacional vinculante que protege al individuo frente a los posibles abusos que entrañe el tratamiento de los datos personales.

El Acuerdo de Adhesión del Reino de España al Convenio de Aplicación del Acuerdo de Schengen de 14 de junio de 1985, entre los gobiernos de los estados de la Unión Económica Benelux, de la República Federal de Alemania y de la República Francesa, relativo a la supresión gradual de los controles en las fronteras comunes, firmado en Schengen el 19 de junio de 1990, al cual se adhirió la República Italiana por el acuerdo firmado en París el 27 de noviembre de 1990, recogía en el punto tercero del Acta Final que: *«Las Partes contratantes toman nota de que el Gobierno del Reino de España se obliga a adoptar, antes de la ratificación del Acuerdo de Adhesión al Convenio de 1990, todas las iniciativas necesarias para que la legislación española sea completada de conformidad con el Convenio del Consejo de Europa de 28 de enero de 1981 para la protección de las personas con relación al tratamiento automatizado de los datos de carácter personal y con observancia de la Recomendación R (87) 15, de 17 de septiembre de 1987 del Comité de Ministros del Consejo de Europa tendente a reglamentar la utilización de los datos de carácter personal en el sector policial, con el fin de dar plena aplicación a las disposiciones de los artículos 117 y 126 del Convenio de 1990 y a las demás disposiciones del Convenio susodicho relativas a la protección de los datos de carácter personal, al objeto de llegar a un nivel de protección compatible con las disposiciones pertinentes del Convenio de 1990.»*

En este intervalo, en agosto de 1990, tras haber promulgado una primera Declaración en el año 1981, la 19ª Conferencia Islámica de El Cairo promulgó la Declaración de los Derechos Humanos en el Islám. Dicho texto que nació con la pretensión de erigirse en alternativa a la Declaración Universal de los Derechos Humanos de la ONU del año 1948, señala en su artículo décimo octavo, apartado b), que:

> *«El Ser humano tiene derecho a la independencia en los asuntos de su vida privada, en su casa, su familia, sus bienes y relaciones. No será lícito espiarlo, someterlo a vigilancia o dañar su reputación. Se le deberá proteger contra toda intromisión arbitraria.»*

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

[20] https://rm.coe.int/informe-explicativo-de-convenio/1680968479

tratamiento de datos personales y a la libre circulación de estos datos, señalaba aún la dicotomía intimidad protección de datos al recoger en su artículo primero que: *«Los Estados miembros garantizarán, con arreglo a las disposiciones de la presente Directiva, la protección de las libertades y de los derechos fundamentales de las personas físicas, y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales.»*

En este sentido, la Carta de los Derechos Fundamentales de la Unión Europea (2000/C364/01)[21] ya hacía una distinción más clara entre privacidad y protección de datos de carácter personal respectivamente en sus artículos 7 y 8.

Como último texto que se pretende citar, estaría el Tratado de Funcionamiento de la Unión Europea[22] (TFUE) que en su artículo 16, también consigna el derecho a la protección de datos con carácter independiente de la siguiente forma:

> *«Artículo 16. (Antiguo artículo 286 TCE)*
>
> *1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.*
>
> *2. El Parlamento Europeo y el Consejo establecerán, con arreglo al procedimiento legislativo ordinario, las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por las instituciones, órganos y organismos de la Unión, así como por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión, y sobre la libre circulación de estos datos. El respeto de dichas normas estará sometido al control de autoridades independientes.*
>
> *Las normas que se adopten en virtud del presente artículo se entenderán sin perjuicio de las normas específicas previstas en el artículo 39 del Tratado de la Unión Europea.»*

Expuesta esta breve cronología del devenir de este derecho, es necesario incidir que en la sociedad actual se ha producido un desarrollo de las tecnologías mediante las que el tratamiento de los datos personales por parte de las personas o entidades que lo realizan, ha alcanzado una extensión formidable y un crecimiento exponencial.

De hecho, siguiendo a Pau. A. y Hernando Grande. A.[23], se podría afirmar que. *«Desde hace un cuarto de siglo, o quizá algo menos, el hombre vive en dos planos: el del mundo físico (que no se puede llamar "el mundo real" porque el otro es tan real como este), y el del cibermundo, ciberespacio o cibercosmópolis.»,* lo que hace actividades humanas que se desarrollan en el mundo físico se desarrollan, también, mutatis mutandis, en el cibermundo o ciberespacio.

Por dicho motivo, debe implantarse la concepción relativa a que los datos personales, tanto en el mundo analógico como en ciberespacio, son parte de la integridad y de la dignidad de las personas de manera que no pueden ser utilizados sin base legal o finalidades que no permitan un conocimiento y valoración clara de las mismas.

---

[21] https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:12016P/TXT&from=DE

[22] https://www.boe.es/doue/2010/083/Z00047-00199.pdf

[23] PAU. A. y HERNANDO GRANDE.A *«La Cibercosmología como premisa del Ciberderecho»* Boletín del Ministerio de Justicia. Nº 2236. Año LXXV. Enero de 2021. NIPO.051-15-001-5

En el campo de las autoridades competentes en el ámbito policial, que principal y mayoritariamente se componen de administraciones públicas, esta potencialidad y desarrollo de instrumentos también se está llevando a cabo, no todo lo rápido que sería deseable, pero de un modo imparable e irreversible. Máxime tras la experiencia vivida durante la gestión de las actuaciones durante la pandemia producida por la Covid-19 y las catástrofes de origen social y natural acaecidas en nuestro país y en Europa.

De hecho, una de las finalidades principales de la normativa de procedimiento administrativo común derivada de la promulgación de las leyes 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas y 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, era su adaptación lo más rápidamente posible a los avances y sistemas de relación e interrelación electrónicos de modo que la tramitación electrónica no fuese todavía una forma especial de gestión de los procedimientos sino que debía constituir la actuación habitual de las Administraciones. Entendía el legislador que una Administración sin papel basada en un funcionamiento íntegramente electrónico no sólo sirve mejor a los principios de eficacia y eficiencia, al ahorrar costes a ciudadanos y empresas, sino que también refuerza las garantías de los interesados. Cuestión ésta claramente discutible si en ese desarrollo no se incluye una cultura de intimidad y protección de los datos.

Esta modernización o digitalización de la administración en esta sociedad tecnificada hace pensar que la Administración Pública será electrónica o no será. Tanto es así que el 9 de marzo de 2021, la Unión Europea ha publicado su *«Digital Compass»*[24]convirtiéndose en un documento detallado donde se incorporan las aspiraciones de lo que se denomina *«la Década Digital de Europa»*.

Esta agenda pretende desarrollar objetivos medibles, concretos y específicos para el objetivo 2030.

Los cuatro ejes principales en torno a los que este programa va a desarrollarse serán:

1. Una ciudadanía capacitada y empoderada digitalmente, así como profesionales del sector, con mayor presencia femenina.
2. Infraestructuras digitales seguras, sostenibles y eficaces.
3. La transformación digital de las empresas.
4. La propia digitalización de los servicios públicos.

Señalando nuevamente que todos estos objetivos deben ir de la mano de unos programas de formación, concienciación e información robustos que faciliten los objetivos de obtención de conocimientos y destrezas en el manejo de estas herramientas digitales y de todo lo que resulta anexo a las mismas entre lo que se encuentra, de manera principal, el dominio de la normativa que protege y garantiza el derecho a la protección de datos de carácter personal.

Por este motivo, cuanto más potencial y más datos se traten, máxime con funciones *«policiales»* mayor nivel de protección y garantías se deben implemen-

[24] https://ec.europa.eu/commission/presscorner/detail/en/ip_21_983

tar en toda su extensión y en todas y cada una de las actividades de tratamiento llevadas a cabo.

Un ejemplo muy reciente que nos puede hacer ver la amplitud del cuidado y sensibilidad que se debe tener consideración es que un estudio llevado a cabo por el INRIA (Instituto Nacional Francés para la Investigación en Ciencia y Automatización)[25] donde se nos muestra que el 96 % de las agencias de seguridad analizadas no eliminaron correctamente los metadatos de documentos en formato pdf antes de publicarlos.

Y, en correspondencia con ello, ya en la década pasada la Agencia Nacional de Seguridad de Estados Unidos (NSA)[26] publicó una guía sobre la seguridad adecuada de documentos electrónicos, recomendando la eliminación de determinada información antes de que un archivo pudiera publicarse y ponerse a disposición de los ciudadanos:

- Metadatos
- Contenido incrustado y archivos adjuntos
- Guiones
- Capas ocultas
- Índice de búsqueda incrustado
- Datos almacenados de formularios interactivos
- Revisiones y comentarios
- Páginas ocultas, imágenes y actualización de datos
- Texto e imágenes oscurecidos
- Comentarios en PDF (no mostrados)
- Datos sin referencias

Consejos y soluciones similares encontramos en las Guías CCN-STIC que son normas, instrucciones, guías y recomendaciones desarrolladas por el Centro Criptológico Nacional (CCN) con el fin de mejorar el grado de ciberseguridad de las organizaciones.

Estas son periódicamente actualizadas y completadas con otras nuevas, en función de las amenazas y vulnerabilidades detectadas y, aunque el grueso de las series está especialmente dirigidas al personal de las Administraciones Públicas y empresas y organizaciones de interés estratégico, otras resultan de difusión pública para todos los usuarios.

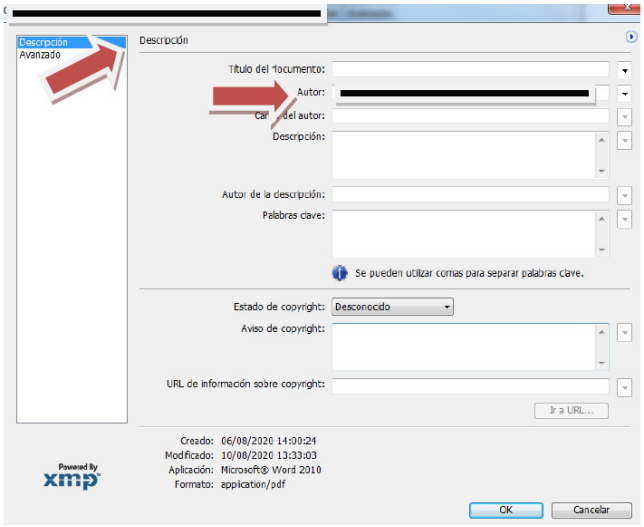
Para comprobar cómo se han implementado estos parámetros en nuestras administraciones podemos navegar hasta las páginas donde se cuelgan los proyectos normativos de cualquiera de nuestros Ministerios y seleccionar el primer archivo documento que aparezca en la página web y chequear las propiedades para observar si obtenemos algún dato personal.

Tras un primer análisis se puede afirmar que muchos de los documentos contrastados conservan aun en sus propiedades datos de esta índole (números de

[25] ADHATARAO. S. y LAURADOUX. C. «Exploitation and Sanitization of Hidden Data in PDFFilesDo Security Agencies Sanitize Their PDF files?» https://arxiv.org/pdf/2103.02707.pdf

[26] https://apps.nsa.gov/iaarchive/library/ia-guidance/security-configuration/index.cfm?page=1

identificación DNI, nombre y apellidos, etc.) lo que nos indica que existe un margen de mejora considerable en las medidas de protección.



En este supuesto incorporado como referencia, en el documento analizado, figuraban el nombre y apellidos completos del autor del mismo, no siendo esto un caso aislado o una excepción[27].

Sin obviar estas obligaciones de las Administraciones Públicas, por otro lado, resulta obligado incidir en que los ciudadanos efectúan un sinfín de actuaciones y utilizan cientos de dispositivos de manera que facilitan muchos de sus datos identificativos a los terceros que los utilizan para unos y otros fines.

Estos fines son o deberían ser conocidos por el público en general, si bien, se puede concluir sin miedo a ser una premisa temería que la mayor parte de los ciudadanos no están informados y no conocen estas acciones y lo que es más relevante, qué se hace con sus datos identificativos.

Pero esto no sólo afecta a los datos que podríamos denominar como propios, sino que, dada la capacidad de la tecnología actual y el uso extensivo que se hace de la misma, se facilita información sobre datos personales (derechos) de terceras personas sin tener tampoco conciencia de ello.

Si por ejemplo analizamos las nuevas etiquetas de seguridad de las *«stores»* digitales[28] muchas aplicaciones recogen cerca del 90 % de los datos potenciales de los interesados que se las instalan y, después, comparten cerca del 80 % con otras entidades o terceros.

---

[27] https://elpais.com/economia/2021-12-10/los-pliegos-de-tres-concursos-publicos-incluian-al-ganador-en-los-metadatos-antes-de-adjudicarse.html

[28] https://blog.pcloud.com/invasive-apps/?s=03

Según información publicada por Andalucía información[29], la empresa pCloud ha utilizado estos datos para analizar una serie de aplicaciones populares en relación con el nivel de datos de los usuarios recogidos y compartidos con terceros con fines comerciales que refleja dentro de las aplicaciones más populares el ratio de datos personales recogidos que se comparten con terceros oscila entre un 21% y un 79%, lo cual no deja de ser significativo.

Como puede apreciarse el uso de Apps y cualquier de los sistemas electrónicos que cotidianamente forman parte de nuestra vida deja una huella o rastro digital en el que figuran identificadores que pueden facilitarles a otros la información sobre nuestra persona, nuestros hábitos, nuestros gustos, nuestra salud, nuestra familia y amigos, etc.

Estos datos o informaciones no son utilizados únicamente de forma local, sino que, debido a la globalización y a las tecnologías de la información, éstos pueden ser objeto de uso a nivel o escala mundial y por un plazo indefinido.

Veamos cómo funcionaría uno de estos sistemas de manera muy simple y resumida (porque la verdad resulta ser un sistema barato y muy potente para los *«usuarios indirectos»* de los datos):

Como se mencionaba, nuestras aplicaciones (APP's) recopilan una infinidad de datos (personales o no) de nuestros dispositivos móviles. Sus ID's de dispositivo único, sus ubicaciones, sus datos demográficos, datos de filiación, edades, etc. De hecho, cada *«Smart TV»* puede estar en contacto con hasta 700 direcciones IP's diferentes durante su uso e incluso en estado de *«stand-by»*.

Los *«agregadores»* de datos obtienen datos de todas las fuentes posibles previo pago en muchas ocasiones. Ej. Cuándo uso mi tarjeta de descuento, cada compra que realizo y me piden un email para mandarme la factura.

Estos *«agregadores»* también denominados *«lectores»* podemos definirlos como los softwares, plataformas web o aplicaciones que almacenan en un solo espacio datos existentes en distintas plataformas digitales. Los tres tipos principales que se utilizan a nivel tecnológico serían los de contenidos, de redes sociales y los financieros.

Todos estos datos agrupados conforman un *«conjunto de datos a la venta»*.

Estos sistemas pueden hacer coincidir mis compras o cualquier actividad con mi cuenta de Twitter, Facebook, Whattapp o cualquier otra App, porque se les ha facilitado a estas entidades la dirección de correo electrónico y el número de teléfono y, además, hemos consentido formalmente todo este intercambio de datos cuando aceptamos sus términos de servicio y las políticas de privacidad. Teniendo en cuenta al mismo tiempo que, estas políticas de privacidad, normalmente son las del lugar de origen o establecimiento de la mercantil donde la protección de datos personales puede tener distinta consideración o extensión (ej. USA, China, Rusia, etc.)

Si nuestros dispositivos se encuentran habitualmente en la misma ubicación GPS que otros teléfonos o terminales, esto queda registrado y se comienza construir la red de personas con las que estamos en contacto habitual.

---

[29] https://andaluciainformacion.es/andalucia/959976/las-apps-que-venden-tus-datos-a-otras-empresas/

Las compañías y entidades pueden hacer referencias cruzadas entre mis intereses, mi historial de navegación y el historial de compras con los intereses de las personas con las que nos relacionamos y comienzan a mostrar diferentes servicios o productos basados en nuestras relaciones en la vida cotidiana. Nos pueden ofrecer estos productos/servicios/información que no queremos o necesitamos, pero saben que alguien con quien estamos en contacto frecuente podría sí quererlo o necesitarlo lo cual conlleva la posibilidad de que en nuestras interrelaciones condicionemos de una manera u otra la conducta de estos terceros. Ej.: *«me ha llegado una publicidad de una película, producto o lugar...y preguntamos al tercero... ¿Tú no querías ver esto o no querías ir a tal sitio? Pues sí, ¿vamos a ver esa película? ¿Te compro está bebida que te gusta?»* Etc.

Como puede observarse es un sistema que simplemente funciona comparando metadatos agregados a través de estos sistemas de muy fácil acceso y, por lo tanto, se puede afirmar que los datos (los que subimos o emitimos desde nuestros dispositivos) no se refieren sólo a nosotros, si no que se trata de cómo se pueden usar en relación con todas las personas que conocemos e incluso con las que no conocemos pero que comparten determinados espacios, actividades, gustos o aficiones con nosotros directamente.

Afectar al comportamiento inconscientemente de las personas es así de sencillo, tratando datos personales sin necesidad de sistemas costosos, «microchips» u otros procedimientos basados en leyendas urbanas, tal y como figuran en el subconsciente colectivo de algunos movimientos sociales.

Pero existen otros muchos ejemplos que nos muestran distintos sistemas de rastreo de datos obtenidos de una aplicación con grave afectación y consecuencias negativas a los derechos de los interesados implicados[30].

Estos aspectos que nos afectan enormemente como interesados, pero parecen no ser tenidos muy en cuenta por la mayoría de los usuarios en aras sencillamente de poder utilizar determinadas herramientas, aplicaciones o sistemas digitales, sin que se valore o se entienda el nivel de riesgo que suponen estas acciones para nuestros derechos fundamentales tanto individuales como colectivos.

En sentido contrario, sí parece que son tenidos muy en cuenta por éstos (*los interesados)* cuando las distintas autoridades competentes tratan datos con distintas finalidades como pueden ser el garantizar estos mismos derechos o protegerlos ante lesiones de terceros; lo cual no deja de ser significativo en cuanto a la preocupación que se derivan de uno u otro tratamiento y la valoración de las garantías que se deben adoptar en un supuesto y en otro.

Se acepta, por ejemplo, el permanecer permanentemente geolocalizados por las empresas sin conocer las finalidades o posibles consecuencias de este hecho y, sin embargo, el ordenamiento exige una auto judicial para localizar a una persona en una actuación donde pueda estar en riego su vida como puede ser una desaparición. Estas son las reglas del juego en un estado democrático de derecho y deben ser cumplidas por todos los operadores públicos y privados.

La utilización de la información pertinente para fines de prevención, investigación y detección de delitos requiere normas específicas sobre protección de

[30] https://apnews.com/article/9f996f24e9cf2be3db112f2ec09eb8e1

datos personales y la libre circulación de los mismos en los ámbitos de la cooperación judicial en materia penal y de la cooperación policial, que están basadas en el citado artículo 16 del TFUE, lo están a razón de la naturaleza específica.

Es forzoso remarcar que la elevada protección otorgada por la legislación especial en este campo, que es el marco competencial de las actuaciones de las autoridades competentes, se aplicará a las personas físicas independientemente de su nacionalidad o lugar de residencia.

Esto no quiere decir que todos los tratamientos que realicen estas Autoridades con otros fines distintos a los señalados se puedan acoger a este régimen especial, puesto que, en la medida en que esté comprendido en el ámbito de aplicación del Derecho de la Unión, entrarán dentro del marco de la normativa específica que resulte oportuna como puede ser el RGPD y las normas dictadas para su adaptación a los derechos internos u otros sectores especiales.

Pero lo que sí tiene que quedar muy asentado (en base al considerando 12 de la Directiva de datos policiales y el artículo 2 del RGPD), es que las actividades de tratamiento de datos realizadas por las Fuerzas y Cuerpos de Seguridad que se centran principalmente en la prevención, investigación o detección de infracciones penales, incluidas las actuaciones policiales en las que no hay constancia de si un incidente es o no constitutivo de infracción penal, las que lleven aparejado el ejercicio de la autoridad mediante medidas coercitivas, como es el caso de las actuaciones policiales en manifestaciones, grandes acontecimientos deportivos y disturbios y otras distintas para mantenimiento del orden público, como labor encomendada a éstas con fines de protección y prevención frente a las amenazas para la seguridad pública quedan fuera de la aplicación del RGPD y están enmarcadas en el régimen especial derivado de la Directiva 680[31].

En concreto, el precitado artículo segundo del RGPD dispone literalmente que este instrumento no se aplique en las siguientes acciones:

- En el ejercicio de una actividad no comprendida en el ámbito de aplicación del Derecho de la Unión (Defensa o Seguridad Nacional, etc.)
- Por parte de los Estados miembros cuando lleven a cabo actividades comprendidas en el ámbito de aplicación del capítulo 2 del título V del TUE.
- Aquellos efectuados por una persona física en el ejercicio de actividades exclusivamente personales o domésticas.
- Los que se efectúen 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.
- Aquellos tratamientos que se lleven a cabo por parte de las instituciones, órganos y organismos de la Unión.

Esta protección de los datos y del derecho fundamental que la soporta (que no posee carácter absoluto como el resto de los derechos), no significa que no se deban

[31] En nuestro caso, 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. https://www.boe.es/buscar/act.php?id=BOE-A-2021-8806

tratar éstos, al contrario, las normas de la Unión tienen un *«apellido»* que parecen olvidar algunos sectores doctrinales. Este es: *«y a la libre circulación de dichos datos»*.

Es decir, la intención de la normativa no es ser un impedimento al tratamiento de los datos o ser un obstáculo, una excusa o un estorbo (*como se suele utilizar, por cierto*) sino ser un instrumento que garantice el nivel adecuado de protección para generar confianza y permitir que las instituciones puedan utilizar y compartir datos para el cumplimiento de sus misiones salvaguardado en cualquier caso todos los derechos en juego.

Confianza, esta sería la palabra o concepto clave que todo responsable de tratamiento y las personas que queden bajo su *«responsabilidad»* deben tener siempre como elemento teleológico en sus actuaciones. Si las personas pueden confiar en las entidades que tienen sus datos porque saben que los van a utilizar únicamente conforme sus fines y a la legalidad, y que las autoridades cumplen con sus obligaciones y tratan los datos de forma ponderada y transparente, el desarrollo de este campo tendrá un enorme futuro y potencial, siendo una herramienta fundamental para el desarrollo de nuestras sociedades democráticas.

La propia Directiva 680/2016, dispone en su considerando 7 que: *«Para garantizar la eficacia de la cooperación judicial en materia penal y de la cooperación policial, es esencial asegurar un nivel uniforme y elevado de protección de los datos personales de las personas físicas y facilitar el intercambio de datos personales entre las autoridades competentes de los Estados miembros...(...)....»;* y en su considerando 15: *«A fin de garantizar el mismo nivel de protección de las personas físicas a través de derechos jurídicamente exigibles en toda la Unión y evitar divergencias que dificulten el intercambio de datos personales entre las autoridades competentes, la presente Directiva debe establecer normas armonizadas para la protección y la libre circulación de los datos personales tratados con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas para la seguridad pública...(...)...»*

En resumen, como axioma se propone la siguiente conclusión:

TRATAMIENTO DE LOS DATOS + CAPACIDAD DE UTILIZARLOS = SERVICIO A LA HUMANIDAD, INNOVACIÓN, CRECIMIENTO Y LOGRO DE OBJETIVOS O MISIONES POR PARTE DE LAS AUTORIDADES COMPETENTES.

De hecho, es importante señalar que según Gago S.[32] la Unión Europea ha puesto en marcha una política estratégica sobre la economía de los datos encaminada a instaurar un mercado único de datos donde la competitividad global y la soberanía de los datos europeos estén garantizadas. Así, muchos consideran la posición de la Unión como el nacimiento de una quinta libertad: la libre circulación de datos.

[32] GAGO. S. *«La Propuesta de Reglamento europeo sobre la gobernanza de los datos y el desarrollo tecnológico europeo.»* LegalToday. Ver en la web: https://www.legaltoday.com/legaltech/novedades-legaltech/la-propuesta-de-reglamento-europeo-sobre-la-gobernanza-de-los-datos-y-el-desarrollo-tecnologico-europeo-2021-08-12/

Piensa la autora que la intención de la Unión es crear un marco europeo seguro de intercambio de datos entre los operadores que intervienen en el mercado: las empresas privadas, el sector público y los interesados de manera que se pueda crear un ambiente adecuado que fomente el surgimiento de empresas europeas que sean capaces de competir con las principales compañías tecnológicas estadounidense o asiáticas gracias al volumen y la variedad de los datos a los que tendrían acceso.

Así, el objetivo marcado tendría su razón de ser en dos elementos principales:

Por un lado, en la protección de los datos personales de sus ciudadanos que ven expuestos, utilizados y/o comercializados en terceros países sin que el beneficio y las ventajas que estos datos reviertan en la Unión y, por otro lado, la necesidad de ser capaces de competir al mismo nivel con esos terceros países con empresas de nacionalidad europea.

Será pues en este contexto técnico-social donde las autoridades competentes deberán ejercer sus cometidos teniendo que desarrollar una importante labor de adaptación al medio para poder cumplir con éxitos sus misiones garantizando los derechos de los ciudadanos y la protección de la seguridad de todos.

2. Situación del derecho a la protección de datos en España

Aunque en el capítulo siguiente se detallará ampliamente como ha quedado el panorama legal en cuanto a la protección de datos en la Unión Europea y particularmente en nuestro país, es necesario recordar en este punto que, siguiendo las bases de los documentos de la OCDE, la legislación específica que ha versado sobre esta materia en nuestro ordenamiento comenzó su andadura con la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal, la cual tenía por objeto limitar el uso de la informática y otras técnicas y medios de tratamiento automatizado de los datos de carácter personal para garantizar el honor, la intimidad personal y familiar de las personas físicas y el pleno ejercicio de sus derechos.

Durante el periplo de la LORTAD se promulgó también la Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos que vino a regular la utilización por las Fuerzas y Cuerpos de Seguridad de videocámaras para grabar imágenes y sonidos en lugares públicos, abiertos o cerrados, y su posterior tratamiento, a fin de contribuir a asegurar la convivencia ciudadana, la erradicación de la violencia y la utilización pacífica de las vías y espacios públicos, así como de prevenir la comisión de delitos, la entonces faltas (delitos leves) y las infracciones relacionados con la seguridad pública.

Esta norma ya hacía una aclaración importante señalando que la captación, reproducción y tratamiento de imágenes y sonidos (datos personales), en los términos previstos en la misma, así como las actividades preparatorias, no se consideraban intromisiones ilegítimas en el derecho al honor, a la intimidad personal y familiar y a la propia imagen, a los efectos de lo establecido en el artículo 2.2 de la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a

la intimidad personal y familiar y a la propia imagen, y que, sin perjuicio de las disposiciones específicas contenidas en la misma, el tratamiento automatizado de las imágenes y sonidos se regiría por lo dispuesto en la propia LORTAD.

La LOV fue desarrollada por el Real Decreto 596/1999, de 16 de abril, por el que se aprobó el Reglamento de desarrollo y ejecución de la misma.

El siguiente paso vino de la mano de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal que superaba la LORTAD y transponía a nuestro ordenamiento el contenido a la Directiva 95/46/CE.

Esta ley orgánica iba un paso más allá en el establecimiento de su ámbito objetivo al establecer su cometido principal en garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar.

En concreto, ésta resultaba de aplicación a los datos de carácter personal registrados en soporte físico, que los hiciera susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado.

Tras casi veinte años de aplicación, en correspondencia con las obligaciones derivadas del bloque de protección de datos de la Unión, con el objetivo de adaptar el ordenamiento jurídico español al RGPD y completar sus disposiciones, se promulgó la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Ésta norma dispone que 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 RGPD y en la misma. Lo cual, como se ha apuntado, no tiene un carácter exhaustivo ni absoluto dado que vamos a estudiar y aplicar otras disposiciones legales que regulan el ejercicio y la protección de este derecho en cada uno de los ámbitos específicos de uso.

En cuanto al ámbito objetivo de aplicación de la LOPDGDD, la norma detalla que 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.

Exceptuando tres grandes bloques de tratamientos de esta esfera: los tratamientos excluidos de aplicación del RGPD por su artículo 2.2[33], los relativos a las personas fallecidas (sin perjuicio de lo establecido en su artículo 3 que posterior-

[33] RGPD. Art.2.2. *«2. El presente Reglamento no se aplica 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 comprendidas 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.»*

mente se detallará) y a los circunscritos en la normativa sobre protección de materias clasificadas.

Dispone esta ley de un régimen de subsidiariedad general, estableciendo que cuando no sea directamente aplicable el RGPD por afectar a actividades no comprendidas en el ámbito de aplicación del Derecho de la Unión Europea, los tratamientos se regirán por lo dispuesto en su legislación específica si la hubiere y supletoriamente por lo establecido en el citado Reglamento y en la propia norma. Encontrándose en esa situación, entre otros, los tratamientos realizados al amparo de la legislación orgánica del régimen electoral general, los tratamientos realizados en el ámbito de instituciones penitenciarias y los tratamientos derivados del Registro Civil, los Registros de la Propiedad y Mercantiles.

De la misma forma, fija que el tratamiento de datos llevado a cabo con ocasión de la tramitación por los órganos judiciales de los procesos de los que sean competentes, así como el realizado dentro de la gestión de la Oficina Judicial, se regirán también por lo dispuesto en el RGPD y está ley orgánica, sin perjuicio de las disposiciones de la Ley Orgánica 6/1985, de 1 julio, del Poder Judicial, que le sean aplicables y de la normas especiales en materia de investigación y enjuiciamiento de infracciones penales.[34]

La LOPDGDD derogó específicamente la anterior LOPD y como el ámbito policial está excluido del RGPD y de la misma, ¿qué normativa se aplicaba entonces en estos supuestos?

Para buscar una solución temporal, el legislador nacional articuló un recurso de transitoriedad ya que, aunque la LOPD figuraba derogada con efectos de 7 de diciembre de 2018, lo estaba sin perjuicio de lo previsto en las disposiciones adicional 14 y transitoria 4 de la Ley Orgánica 3/2018, de 5 de diciembre, según establecía el contenido de su disposición derogatoria única.

Disposiciones éstas que respectivamente establecieron que toda esta ley en su conjunto continuaba vigente para los tratamientos policiales hasta que se produjese la transposición de la Directiva 680/2016, de 27 de abril, y por lo tanto, en el caso de lagunas o necesidad de interpretación, habría de acudir a la posible aplicación del efecto directo horizontal del contenido de la propia Directiva y, subsidiariamente, al RGPD, la LOPDGDD y al resto de instrumentos de los que nos dota nuestro sistema legal para cubrir las posibles lagunas normativas.

Es interesante incidir en este punto porque muchas entidades entendieron que permanecían vigentes sólo algunos artículos de la LOPD (artículos 22 y siguientes) y de su reglamento de desarrollo[35], si bien, esa no fue la intención del legislador ya que en las citadas disposiciones transitoria 4 y adicional decimocuarta de la LOPDGDD, establecían respectiva y literalmente lo siguiente:

> *«Los tratamientos sometidos a la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por*

[34] Vid. la Disposición final segunda y tercera de la LOPDP.

[35] 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

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 y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo, continuarán rigiéndose por la Ley Orgánica 15/1999, de 13 de diciembre, y en particular el artículo 22, y sus disposiciones de desarrollo, en tanto no entre en vigor la norma que trasponga al Derecho español lo dispuesto en la citada directiva.»

«Las normas dictadas en aplicación del artículo 13 de 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, que hubiesen entrado en vigor con anterioridad a 25 de mayo de 2018, y en particular los artículos 23 y 24 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, siguen vigentes en tanto no sean expresamente modificadas, sustituidas o derogadas.»

En este intervalo, originaria de la transposición de la Directiva PNR, se aprobó la Ley Orgánica 1/2020, de 16 de septiembre, sobre la utilización de los datos del Registro de Nombres de Pasajeros para la prevención, detección, investigación y enjuiciamiento de delitos de terrorismo y delitos graves con el objetivo de regular:

- La transferencia de datos de los datos PNR, así como de la información de las tripulaciones correspondientes a vuelos internacionales y, en su caso, nacionales, en los términos y a los efectos previstos en el misma.
- El sistema de recogida, uso, almacenamiento, tratamiento, protección, acceso y conservación de los datos PNR, la transmisión de dichos datos a las autoridades competentes, así como el intercambio de los mismos con los Estados miembros de la Unión Europea, con Europol y con terceros países.
- La determinación y atribución de las funciones de la Unidad de Información sobre Pasajeros española situada en el CITCO.
- El régimen sancionador aplicable.

El siguiente paso dado fue el 9 de marzo de 2021, cuando el Consejo de Ministros acordó solicitar la tramitación parlamentaria por el procedimiento de urgencia del proyecto de Ley Orgánica de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.

Tras el correspondiente trámite parlamentario, el día 26 de mayo del mismo año, se aprobó la Ley Orgánica 7/2021, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, que entró en vigor el 16 de junio siguiente.

Esta LOPDP tiene por objeto establecer las normas específicas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos de carácter personal por parte de las autoridades competentes, con fines de prevención, detección, investigación y enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y prevención frente a las amenazas contra la seguridad pública.

Siguiendo lo dispuesto en la LOPDGDD, 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, realizado por las autoridades competentes para los fines señalados (elemento clave en nuestra opinión)

De hecho, lo hace siguiendo el considerando 18 de la propia DDP y el artículo 3, que vienen a especificar que:

> *«Para evitar que se produzcan graves riesgos de elusión, la protección de las personas físicas debe ser tecnológicamente neutra y no debe depender de las técnicas utilizadas. La protección de las personas físicas debe aplicarse al tratamiento automatizado de los datos personales, así como a su tratamiento manual si los datos personales están contenidos o destinados a ser incluidos en un fichero. Los ficheros o conjuntos de ficheros y sus portadas que no estén estructurados con arreglo a criterios específicos no deben incluirse en el ámbito de aplicación de la presente Directiva»*

Fija asimismo el régimen de las Autoridades judiciales y fiscales en las actuaciones o procesos en lo que sean competentes en este marco, así como el realizado dentro de la gestión de la Oficina judicial y fiscal, al determinar que será esta ley orgánica la que se aplique sin perjuicio de las disposiciones de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, la Ley 50/1981, de 30 de diciembre, por la que se regula el Estatuto Orgánico del Ministerio Fiscal y las leyes procesales que le sean aplicables. En correspondencia con lo cual, es importante reflejar que en las disposiciones finales segunda y tercera de la LOPDP se han incorporado modificaciones sustanciales a dichas normas en materia de protección de datos.

También excluye de su ámbito de aplicación determinados tratamientos que se enumeran a continuación:

- Los realizados por las autoridades competentes para fines distintos de los previstos en su artículo 1 (prevención, detección, investigación y enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y prevención frente a las amenazas contra la seguridad pública), incluidos los fines de archivo por razones de interés público, investigación científica e histórica o estadísticos. Estos tratamientos se someterán plenamente a lo establecido en el RGPD, así como en la LOPDGDD.
- Los llevados a cabo por los órganos de la Administración General del Estado en el marco de las actividades comprendidas en el ámbito de aplicación del capítulo II del título V del Tratado de la Unión Europea.
- Los tratamientos que afecten a actividades no comprendidas en el ámbito de aplicación del Derecho de la Unión Europea.
- Los sometidos a la normativa sobre materias clasificadas, entre los que se incluyen los relativos a la Defensa Nacional.
- Los tratamientos de datos de personas fallecidas.

En cuanto a la aplicación subjetiva, la norma establece quiénes se considerarán autoridades competentes a sus efectos:

Éstas serán toda autoridad *«pública»* que tenga competencias o misiones directas y específicas encomendadas legalmente para el tratamiento de datos personales con alguno de los fines previstos.

Como puede apreciarse, no se establece un *«numerus clausus»* de autoridades, si bien señala que en particular tendrán esta consideración, en el ámbito de sus respectivas competencias específicas, las siguientes:

- Las Autoridades judiciales del orden jurisdiccional penal y el Ministerio Fiscal.
- Las Fuerzas y Cuerpos de Seguridad.
- Las Administraciones Penitenciarias.
- La Dirección Adjunta de Vigilancia Aduanera de la Agencia Estatal de Administración Tributaria.
- El Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias.
- La Comisión de Vigilancia de Actividades de Financiación del Terrorismo.

En correspondencia con esta definición se han planteado algunas dudas por parte de algunos profesionales en base a sí la finalidad de ejecutar las sanciones penales incluía a las autoridades no propiamente penitenciarias que tratan datos de menores a los que se les pudiera exigir responsabilidad por la comisión de hechos tipificados como infracciones penales en el Código Penal o en las leyes penales especiales. Ante esta cuestión se puede valorar que el legislador utiliza la formula «sanciones penales» y no penas como se dispone en el artículo 32 del Código Penal con la finalidad de incluir las medidas incorporadas en el artículo 7 de la Ley Orgánica 5/2000, de 12 de enero, reguladora de la responsabilidad penal de los menores.

Si el organismo en cuestión es una administración pública y ésta posee competencias directas y específicas (no genéricas[36]) para cumplimiento de estos fines, se pueden entender que para estos tratamientos si deberían tener la consideración de autoridades competentes.

En cuanto a las *«categorías de interesados»* titulares de los datos personales la DDP en su considerando 31 venía a explicar que en este campo se pueden tratar

[36] La competencia debe entenderse restringida y referida directa y específicamente al cumplimiento de estos fines porque es la finalidad y el propósito de los legisladores, tanto europeos como internos, ya que a nivel indirecto o no exclusivo, casi la totalidad de las entidades públicas tienen obligaciones genéricas de prevenir o detectar delitos (delitos fiscales, delitos de seguridad social, riesgos laborales, *«corporate compliance»*, alertadores, obligación de denunciar cuando se observe cualquier delito público, etc.) y además pueden participar en procesos penales o actividades derivados de los mismos sin formar parte del proceso (protección social de las víctimas, tratamiento de resarcimientos, embargos, etc...)

Del mismo modo, el contenido del artículo 2 de la LOPDP excluye varios supuestos del ámbito de aplicación, en concreto en los apartados 2.3.1: *«Los realizados por las autoridades competentes para fines distintos de los previstos en el artículo 1, incluidos los fines de archivo por razones de interés público, investigación científica e histórica o estadísticos. Estos tratamientos se someterán plenamente a lo establecido 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 por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos), así como en la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales.»,* y el artículo 2.3. e) que señala: *«Los tratamientos realizados en las acciones civiles y procedimientos administrativos o de cualquier índole vinculados con los procesos penales que no tengan como objetivo directo ninguno de los fines del artículo 1.»* Clarificando de ese modo esta cuestión.

estos datos siendo relativos a diferentes tipos de personas. Por ello, si procede y siempre que sea posible, se deben diferenciar claramente los datos personales de los distintos interesados, tales como los sospechosos, los condenados por una infracción penal, las víctimas o los terceros, entre los que se incluyen los testigos, las personas que posean información o contactos útiles y los cómplices de sospechosos y delincuentes condenados.

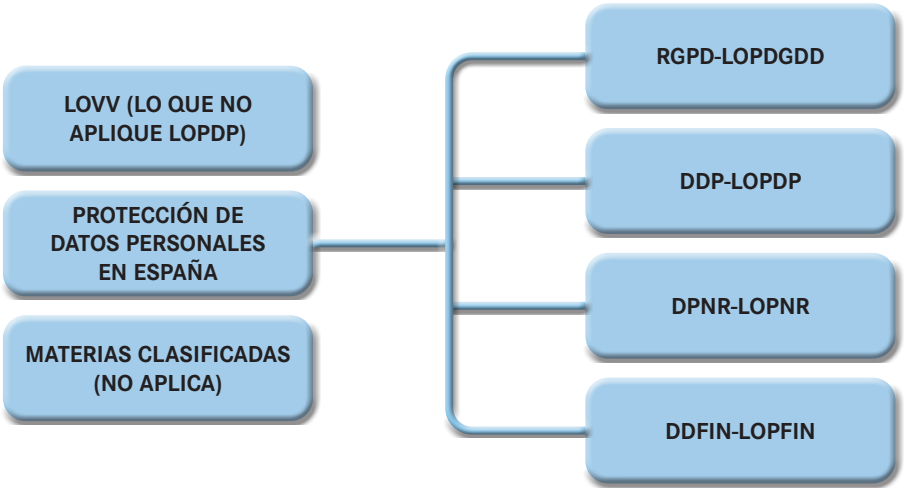
Lo anterior, aunque esto pudiera ser una obviedad en un sistema democrático como el nuestro, se aplicará de forma que no se impida la aplicación del derecho a la presunción de inocencia.

El legislador español, en base a este considerando 31 y al contenido del artículo 6, incorporó dicha previsión en la LOPDP señalando que, en la medida de lo posible, la autoridad competente responsable del tratamiento establecerá entre los datos personales de las distintas categorías de interesados, distinciones tales como:

- Personas respecto de las cuales existan motivos fundados para presumir que hayan cometido, puedan cometer o colaborar en la comisión de una infracción penal.
- Personas condenadas o sancionadas por una infracción penal.
- Víctimas o afectados por una infracción penal o que puedan serlo.
- Terceros involucrados en una infracción penal o un tratamiento comprendido en punto primero, como son, personas que puedan ser citadas a testificar en investigaciones relacionadas con infracciones o procesos penales ulteriores, personas que puedan facilitar información sobre dichas infracciones, o personas de contacto o asociados de una de las personas mencionadas en los dos primeros puntos.

Se puede observar que no es una lista cerrada, si bien agrupa la mayoría de los supuestos que pueden concurrir en los tratamientos de las autoridades competentes con los fines previstos.

¿Cuál sería la imagen panorámica del sistema específico actual en nuestro país? Podría valorarse a simple vista en el siguiente cuadro:



II. CONSTITUCIÓN ESPAÑOLA. PRIVACIDAD, DERECHOS A LA INTIMIDAD, AL HONOR, A LA PROPIA IMAGEN Y A LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

1. Constitución española

La Carta Magna viene a recoger en su artículo 18.1., y 4, lo siguiente:

> *«1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.*
> *...(...)...*
> *4. 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.»*

Como se apuntaba previamente, la LOPDGDD dispone en su exposición de motivos y en su artículo 1, que:

> *«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.»*

Puede apreciase que el apartado 1 del precitado precepto constitucional, que salvaguarda los derechos al honor, la intimidad y la propia imagen no recoge el derecho a la protección de datos personales que resulta ser un derecho autónomo e independiente y con el mismo estatus de los otros tres referidos que viene a incardinarse en su apartado 4.

Aunque en un primer momento esta protección de los datos frente al uso de la informática en nuestra Constitución deriva de la apreciación de los peligros que puede entrañar el archivo y uso ilimitado de los datos informáticos; nuestros constituyentes concienciados del desarrollo de esta tecnología, siguieron el ejemplo de la Constitución portuguesa, sólo dos años anterior a la española, y lo reflejaron específicamente en este precepto. Si bien, al hablar del derechos al protección de datos, aunque en un principio iba irremediablemente unido al derecho a la intimidad, nos encontramos ante un derecho fundamental por el que se garantiza a la persona el control sobre sus datos, cualesquiera datos personales, y sobre su uso y destino, para evitar el tráfico ilícito de los mismos o lesivo para la dignidad y los derechos de los afectados; de esta forma, se configura en este momento como una facultad del ciudadano para oponerse a que determinados datos personales sean simplemente usados o que sean utilizados para fines distintos a aquellos que justificaron su obtención.

Este derecho alcanzaría dicho estatus *«pacificado»* derivado principalmente de la interpretación del apartado 4 que hizo el Tribunal Constitucional en sus sentencias STC 254/1993, de 20 de julio y 290/2000, de 30 de noviembre.

Es muy importante el determinar la extensión y alcance de cada derecho puesto que, aunque podemos hablar de derechos muy relacionados, cada uno tiene unos presupuestos y una extensión propia que resulta oportuno conocer ya

que se derivan consecuencias y situaciones muy diferentes a la hora de su aplicación o su ejercicio.

A modo de ejemplo, la propia Constitución, en relación con los derechos y libertades recogidos en su artículo 20 (en concreto la libertad de expresión y de información, el derecho a la producción y creación literaria, artística, científica y técnica y el referido a la libertad de cátedra), fija sus límites en los preceptos de las leyes que lo desarrollen y, especialmente, en el derecho al honor, a la intimidad, a la propia imagen y a la protección de la juventud y de la infancia y, de conformidad con lo dispuesto en el artículo 55, entiende que determinados derechos (entre ellos los recogidos en este artículo 18) podrán ser suspendidos cuando se acuerde la declaración del estado de excepción o de sitio en los términos previstos en la Constitución.

Esto no podría entenderse ni llevarse a cabo sin que por parte de las distintas autoridades y órganos del Estado se conociera cual es el ámbito objetivo y subjetivo de aplicación de estos diferentes derechos.

Analizando el contenido de la Sentencia 290/2000, de 30 de noviembre, del TC,[37]si nos centramos en su fundamento de derecho séptimo, observamos el contenido que el Alto Tribunal establece para el mismo:

> *«En lo que respecta al primer presupuesto, si el art. 1 L.O.R.T.A.D. establece que su objeto es el "desarrollo de lo previsto en el apartado 4 del art. 18 C.E.", es procedente recordar que este precepto, como ya ha declarado este Tribunal, contiene un instituto de garantía de los derechos a la intimidad y al honor y del pleno disfrute de los restantes derechos de los ciudadanos que es, además, en sí mismo, "un derecho fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento automatizado de datos, lo que la Constitución llama 'la informática'" (STC 254/1993, de 20 de julio, F.J. 6, doctrina que se reitera en las SSTC 143/1994, de 9 de mayo, F.J. 7; 11/1998, de 13 de enero, F.J. 4; 94/1998, de 4 de mayo, F.J. 6, y 202/1999, de 8 de noviembre, F.J. 2).*
>
> *De este modo, en cuanto desarrollan el mandato del art. 18.4 C.E., las previsiones de la L.O.R.T.A.D. limitando el uso de la informática están estrechamente vinculadas con la salvaguardia de ese derecho fundamental a la protección de datos personales frente a la informática o, si se quiere, a la "libertad informática" según la expresión utilizada por la citada STC 254/1993. Y cabe agregar, además, que en esta decisión ya hemos hecho referencia al aspecto institucional de tales previsiones al señalar que, tras la aprobación de la L.O.R.T.A.D., "la creación del Registro General de Protección de Datos, y el establecimiento de la Agencia de Protección de Datos, facilitarán y garantizarán el ejercicio de los derechos de información y acceso de los ciudadanos a*

[37] Recursos de inconstitucionalidad acumulados 201/93, 219/93, 226/93 y 236/93. Promovidos por el Consejo Ejecutivo de la Generalidad de Cataluña, el Defensor del Pueblo, el Parlamento de Cataluña y por don Federico Trillo-Figueroa Conde, Comisionado por 56 Diputados del Grupo Parlamentario Popular, contra diversos artículos de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal. Competencia sobre derechos fundamentales y la Agencia de Protección de Datos. Voto particular. https://www.boe.es/buscar/doc.php?id=BOE-T-2001-330

los ficheros de titularidad pública, y además extienden su alcance a los de titularidad privada" (Ibid, F.J. 10).

En efecto, ha de tenerse presente, como ya se anticipaba en la decisión de este Tribunal que se acaba de mencionar, que el derecho fundamental al que estamos haciendo referencia garantiza a la persona un poder de control y disposición sobre sus datos personales. Pues confiere a su titular un haz de facultades que son elementos esenciales del derecho fundamental a la protección de los datos personales, integrado por los derechos que corresponden al afectado a consentir la recogida y el uso de sus datos personales y a conocer los mismos. Y para hacer efectivo ese contenido, el derecho a ser informado de quién posee sus datos personales y con qué finalidad, así como el derecho a oponerse a esa posesión y uso exigiendo a quien corresponda que ponga fin a la posesión y empleo de tales datos.

En suma, el derecho fundamental comprende un conjunto de derechos que el ciudadano puede ejercer frente a quienes sean titulares, públicos o privados, de ficheros de datos personales, partiendo del conocimiento de tales ficheros y de su contenido, uso y destino, por el registro de los mismos. De suerte que es sobre dichos ficheros donde han de proyectarse, en última instancia, las medidas destinadas a la salvaguardia del derecho fundamental aquí considerado por parte de las Administraciones Públicas competentes.»

Estos presupuestos del TC son de aplicación constante por parte de nuestros juzgados y tribunales, en concreto, resulta habitual encontrarlos en sentencias del Tribunal Supremo[38].

A modo de ejemplo, la STS 3118/2020[39], dispone:

«Según declara la STC 292/2000, de 30 de noviembre, el derecho reconocido en el artículo 18.4 CE "[...] contiene, en los términos de la STC 254/1993, un instituto de garantía de los derechos a la intimidad y al honor y del pleno disfrute de los restantes derechos de los ciudadanos que, además, es en sí mismo 'un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos, lo que la Constitución llama la informática', lo que se ha dado en llamar 'libertad informática' (FJ 6, reiterado luego en las SSTC 143/1994, FJ 7 , 11/1998, FJ 4, 94/1998, FJ 6, 202/1999, FJ 2). La garantía de la vida privada de la persona y de su reputación poseen hoy una dimensión positiva que excede el ámbito propio del derecho fundamental a la intimidad (art. 18.1 CE), y que se traduce en un derecho de control sobre los datos relativos a la propia persona. La llamada 'libertad informática' es así derecho a controlar el uso de los mismos datos insertos en un programa informático ('habeas data') [...]".

Resulta igualmente muy clarificador el último informe de Naciones Unidas (Consejo de Derechos Humanos) denominado "*The right to privacy in the digital age*"[40] donde se dispone que el derecho a la privacidad es una

[38] Vid. STS 743/2021 - ECLI:ES:TS:2021:743. Id Cendoj: 28079120012021100156. STS 832/2021 - ECLI:ES:TS:2021:832. Id Cendoj: 28079120012021100182

[39] STS 3118/2020 - ECLI: ES:TS:2020:3118, Id Cendoj: 28079120012020100513

[40] A/HRC/48/31, "The right to privacy in the digital age*"13 September-1 October 2021. Annual report of the United Nations High Commissioner for Human Rights and reports of the

> expresión de la dignidad humana y está vinculado a la protección de la autonomía humana y la identidad personal. Los aspectos de la privacidad que son de particular importancia en el contexto del uso de la Inteligencia Artificial incluyen la privacidad de la información, que abarca la información que existe o puede derivarse sobre una persona y su vida y las decisiones basadas en esa información y la libertad de tomar decisiones sobre la propia identidad.»

2. Privacidad. Derecho a la intimidad, Derecho al Honor, Derecho a la propia imagen y Derecho a la protección de datos personales

Como se señalaba en el apartado anterior los conceptos a manejar por las personas con responsabilidades en materia de protección de datos personales son diversos y diferentes.

Para poder aplicar las distintas normas se ha de producir cierta actividad de interpretación en mayor o menor extensión[41], la cual, en su momento final, corresponde a los Juzgados y Tribunales. No obstante, hasta que estas instancias llegan a dar pacíficamente su valoración, son los distintos agentes que tratan los datos personales y las autoridades independientes de control los que van a realizar dicho ejercicio en la aplicación y de definición del contenido.

El artículo 3.1 del Código Civil viene a disponer que:

> *«Las normas se interpretarán según el sentido propio de sus palabras, en relación con el contexto, los antecedentes históricos y legislativos, y la realidad social del tiempo en que han de ser aplicadas, atendiendo fundamentalmente al espíritu y finalidad de aquellas»*

Hacer un análisis exhaustivo de los derechos citados excedería con mucho el contenido de ésta y otras obras, pero es importante mencionar algunas ideas básicas que nos ayuden a diferenciar los distintos elementos a proteger y conceptos a desarrollar para un mejor cumplimiento de las misiones a llevar a cabo.

Desde el punto de vista del sentido propio de las palabras podemos acudir al Diccionario de la Real Academia[42] que define los siguientes conceptos:

Confidencialidad: *«1. adj. Que se hace o se dice en la confianza de que se mantendrá la reserva de lo hecho o lo dicho.»*

Privacidad: *«1. f. Cualidad de privado. 2. f. Ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión. Privado: Del part. de privar; lat. privātus. 1. adj. Que se ejecuta a vista de pocos, familiar y domésticamente, sin formalidad ni ceremonia alguna. 2. adj. Particular y personal de cada individuo....(...)»*

Office of the High Commissioner and the Secretary-General. Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development.

[41] CELSO (D.1.3.17): «*scirelegesnon hoc est verbaearumtenere, sed vim ac potestatem*»; o lo que es lo mismo, conocer las leyes no consiste solo en entender sus palabras sino en comprender su fin y sus efectos.

[42] https://dle.rae.es/

Intimidad: *«1. f. Amistad íntima. 2. f. Zona espiritual íntima y reservada de una persona o de un grupo, especialmente de una familia.»*

Protección de datos: *«1. f. Sistema legal que garantiza la confidencialidad de los datos personales en poder de las Administraciones públicas u otras organizaciones.»*

Asimismo, en el Diccionario del Español Jurídico[43], que hace una interpretación algo diferente de estos conceptos que resulta interesante incluir:

Confidencial: *«1.Gral. Que se dice o se hace en confianza, con seguridad recíproca de dos o más personas. 2. Adm. Dicho de cualquier dato personal: Que no puede ser divulgado ni comunicado a tercero.»*

Privacidad: *«1. Gral. Facultad de una persona de prevenir la difusión de su vida privada que, sin ser difamatorios o perjudiciales, esté desea que no desea que no sean divulgados.»*

Intimidad: «Ámbito reservado de una persona o una familia. Derecho a la intimidad: Derecho a disfrutar de un ámbito propio y reservado para desarrollar una vida personal y familiar plena y libre, excluido tanto del conocimiento como de las intromisiones de terceros.»

Protección de datos: *«Adm. Conjunto de medidas para garantizar y proteger los datos de carácter personal (cualquier información concerniente a personas físicas identificadas o indentificables) registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado, a los efectos de garantizar y proteger las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar.»*

Derecho a la Protección de datos: *«Const. Derecho fundamental de toda persona física que la faculta para disponer y controlar sus datos de carácter personal, pudiendo decidir cuales proporcionar a terceros, así como conocer quién posee esos datos y para qué, y oponerse a esa posesión o tratamiento.»*

Más allá de estas definiciones gramaticales o conceptuales, se puede y se debe acudir a las definiciones, ejemplos y aproximaciones a los distintos conceptos que hacen los órganos y organismos especializados, entre los que se encuentran el Tribunal Europeo de los Derechos Humanos[44], el Tribunal de Justicia de la Unión Europea, nuestros Tribunales, las Autoridades independientes de Control (de carácter nacional o internacional) como la Agencia Española de Protección de Datos, las Autoridades Autonómicas de Protección de Datos, el extinto Grupo de Trabajo del Artículo 29 (WP29), el Comité Europeo de Protección de Datos (CEPD)[45], el Supervisor Europeo de Protección de Datos (SEPD)[46] y el Delegado de protección de datos de la Comisión Europea.[47]

---

[43] https://dpej.rae.es/

[44] Resulta de suma importancia la *«Guide to the Case-Law of the of the European Court of Human Rights»* del Tribunal Europeo de los Derechos Humanos (updated on 30 April 2021) donde se recogen las definiciones básicas y los principios de la protección de datos personales y un listado de su Jurisprudencia sobre esta materia.

[45] https://edpb.europa.eu/edpb_es

[46] https://edps.europa.eu/_en?lang=es

[47] La Comisión Europea ha nombrado un delegado de protección de datos responsable de supervisar la aplicación de las normas sobre protección de datos en la Comisión Europea. El

Dada la importancia de este órgano, señalamos que el CEPD está compuesto por representantes de las autoridades nacionales de protección de datos de los Estados Miembros y asociados y del SEPD y cumple con las funciones que antes realizaba el WP29, constituyéndose como el organismo independiente que contribuye a la aplicación coherente de las normas de protección de datos en toda la Unión Europea y promueve la cooperación entre las autoridades de protección de datos de los Estados Miembros. Es decir, entre otras muchas funciones, garantiza la aplicación coherente del RGPD y la Directiva europea sobre protección de datos en el ámbito policial, pudiendo adoptar directrices generales para clarificar los términos de la legislación europea de protección de datos, proporcionando a todas las partes interesadas una interpretación coherente de sus derechos y obligaciones.

Por dicho motivo, es importante acudir a sus informes, guías y dictámenes para clarificar el significado de los conceptos normativos (DPD, tratamientos masivos, conceptos de responsable y encargado, etc.), buscar ejemplos, etc.

Cobran especial importancia sus «Directrices», «Recomendaciones», «Buenas Prácticas» y otros documentos como los antiguos informes del WP29 que ahora ha hecho suyos y ratificado su contenido.

Es relevante conocer su primer documento en el ámbito policial, como son las *«Recommendations 01/2021 on the adequacy referential under the Law Enforcement Directive.» (Recomendaciones 01/2021 relativas a las referencias sobre adecuación en el marco de la Directiva sobre protección de datos en el ámbito penal),* de 2 de febrero de 2021, con traducción oficial[48], que viene a clarificar el concepto o nivel de adecuación apropiado en materia de protección de datos cuando se deban realizar transferencias internacionales que queden bajo el amparo de la DDP.

De la misma forma, el SEPD tiene como función el garantizar que, a la hora de tratar datos personales, las instituciones y organismos de la UE respeten el derecho a la intimidad (que habría que extender al derecho a la protección de datos) de los ciudadanos. Este organismo supervisa el tratamiento de los datos personales por parte de la administración de la UE, a fin de garantizar el cumplimiento de las normas de protección de la intimidad, asesora a las instituciones y los organismos de la UE sobre todo lo relativo al tratamiento de los datos personales y las políticas y legislación al respecto, se ocupa igualmente de las reclamaciones, realiza investigaciones, colabora con las autoridades nacionales de la UE para garantizar la coherencia en la protección de datos y supervisa las nuevas tecnologías que puedan tener una incidencia en la protección de datos.

Si alguna persona interesada considera que una institución u organismo de la UE ha violado su derecho a la protección de datos, se debe dirigir a los responsables del tratamiento de tus datos en el servicio donde se produce la posible anomalía y si no queda satisfecho con su respuesta o entiende que debe recurrirse, puede presentar una reclamación ante el SEPD, quien llevará a cabo una investigación y le comu-

---

delegado de protección de datos garantiza de manera independiente la aplicación interna de las normas, en cooperación con el Supervisor Europeo de Protección de Datos. Ver en la página web: https://ec.europa.eu/info/departments/data-protection-officer_es

[48] https://edpb.europa.eu/system/files/2021-05/recommendations012021onart.36led.pdf_es.pdf

nicará si está de acuerdo con la reclamación, informándole de las medidas que haya podido adoptar para corregir la situación. Ante esta decisión del SEPD, se puede llevar el asunto ante el Tribunal de Justicia de la UE lo que supone una herramienta muy potente para garantizar la correcta aplicación del derecho de la Unión.

Una muestra de actuación de estos órganos que puede afectar a funciones de las FCS (aunque no tengan por finalidad las del artículo 1 de la LOPDP), nos la encontramos con el dictamen conjunto sobre las propuestas de certificado verde digital en la U.E.[49] Con dicha decisión, el EDPB y el SEPD invitan a los colegisladores a garantizar que el certificado verde digital se ajusta plenamente a la legislación de la UE en materia de protección de datos personales. Los comisionados de protección de datos de todos los países de la UE y del Espacio Económico Europeo destacan la necesidad de mitigar los riesgos para los derechos fundamentales de los ciudadanos y residentes de la UE que pueden resultar de la emisión del Certificado Verde Digital, incluidos sus posibles usos secundarios no deseados. El EDPB y el SEPD subrayan en este documento que el uso del Certificado Verde Digital no puede, en modo alguno, dar lugar a una discriminación directa o indirecta de las personas y debe estar plenamente en consonancia con los principios fundamentales de necesidad, proporcionalidad y eficacia. Dada la naturaleza de las medidas propuestas consideraban que la introducción del Certificado Verde Digital debería ir acompañada de un marco jurídico global.

Del mismo modo, la AEPD y las autoridades autonómicas poseen un buen número de herramientas que dotan a los distintos operadores y agentes implicados de directrices, guías, interpretaciones, definiciones, recomendaciones, aplicaciones, sede electrónica y canales de comunicación que facilitan mucho la aplicación y el cumplimiento de la normativa.

Es por ello que resulta inexcusable, al menos, la visita y el conocimiento de lo recogido en la página web de la AEPD[50] en cada una de sus secciones.

En relación con las definiciones, la AEPD en su blog ha empezado también a traer a colación y emplear cotidianamente nuevos conceptos como el de pruebas de conocimiento cero, IoT (Internet of Things), blockchain desde la protección datos, privacidad de grupo, etc.

Este último concepto, el de privacidad de grupo, como novedad interesante y poco conocida, la describe como:

> *«....la privacidad correspondiente a grupos definidos por cualquier característica o combinación de características que se asocian a determinados individuos.*
>
> *El perfilado de las personas y su tratamiento por, por ejemplo, el Estado o los servicios de Internet, se puede considerar uno de los riesgos más importantes a la privacidad. El enfoque de la privacidad tomando al individuo de forma aislada tiene un origen histórico, puesto que el nivel tecnológico limitaba en el pasado las posibilidades del tratamiento masivo de datos de la población. Sin embargo, el avance de las técnicas de tratamiento de la información, como las*

[49] EDPB-EDPS Joint Opinion 04/2021 on the Proposal for a Regulation of the European Parliament and of the Council on a framework for the issuance, verification and acceptance of interoperable certificates on vaccination, testing and recovery.

[50] https://www.aepd.es/es

de Big Data o Inteligencia Artificial, ha introducido nuevos aspectos a tener en cuenta. Según el filósofo Luciano Floridi, la mayoría de las personas no están perfiladas como individuos, sino como miembros de un grupo específico, y no se da la relevancia adecuada a las amenazas que de ello se derivan. ...(...)....

En este sentido, la constitución de un grupo permite la aplicación de lo que se denomina "conocimiento generalizable", que implica universalizar a todos los miembros ciertas características comunes solo a alguno de ellos. Por ejemplo, el conocimiento generalizable de que fumar causa cáncer expone a todos los fumadores a precios de seguros médicos más altos.

Estos tratamientos conllevan riesgos para los individuos, no sólo por su inclusión implícita en un grupo del que no tiene conocimiento, sino de que hay decisiones que le afectan y puede verse afectado por sesgos de los que se desconoce su alcance y posibles consecuencias. Podríamos encontramos con resultados discriminatorios por razón de género, raza, opiniones, hábitos o localizaciones geográficas concretas. Los miembros de un grupo se podrían ver atacados o discriminados sin que ellos mismos lo sepan... (...) ....

Una conclusión importante es la concienciación de los individuos sobre la importancia de preservar la propia privacidad, que va más allá de las consecuencias que puede tener para su propia privacidad sino también puede afectar a los derechos y libertades de la sociedad en su conjunto. Esto no es un impedimento para los innumerables potenciales de la tecnología, sino más bien una condición para que este potencial se lleve a cabo de una manera responsable.»[51]

Como hemos visto, esta noción es una concepción interesante que está ligada a la posible afectación a terceros que se ha analizado y sobre la que el Gabinete Jurídico de la AEPD ha dictado el importante informe 35/2021[52], donde, aunque recoge que el Reglamento general de protección de datos no aborda de manera explícita la *«privacidad de grupo»* refleja que la adopción de las medidas técnicas y organizativas adecuadas en orden a la mejor garantía de la protección de los datos de carácter personal de los potenciales afectados —con pleno respeto de los principios del artículo 5 del RGPD, especialmente a los de limitación de la finalidad y minimización de datos —, se refiere a los datos de personas físicas identificadas y/o identificables. Si olvidar, por otro lado, que lo que *«sí resulta necesario es la adopción de las medidas necesarias para evitar los riesgos que permitan identificar a las personas físicas individualizadas que forman parte del grupo, así como la posibilidad de asignar a las mismas el sentido de su voto, que supondría el tratamiento de un dato personal en principio prohibido por el artículo 9 del RGPD, tal y como se analizará posteriormente.»*

Sin perjuicio de lo apuntado hasta este punto, en cuanto al concepto social actual de intimidad y privacidad habría que analizar este aspecto con sumo cuidado puesto que las generaciones que comparten este tramo de la historia tienen o asumen de manera muy diferente estas acepciones en función de lo que utilicen o se manejen en el mundo de las TIC's.

[51] «Privacidad de grupo» 19 octubre de 2020, AEPD https://www.aepd.es/es/prensa-y-comunicacion/blog/privacidad-de-grupo

[52] https://www.aepd.es/es/documento/2021-0035.pdf

El filósofo Zygmunt Bauman, en el estudio de lo que denominaba la modernidad líquida hacía observaciones muy interesantes sobre la apreciación de estos conceptos en la sociedad actual tales como:

- *«El miedo a ser observado ha sido vencido por la alegría de ser noticia»*
- La pesadilla orwelliana del nunca estoy solo *«ha sido refundida pen la esperanza de no volver a estar solo, excluido, ignorado, olvidado.»*
- *«Para entrar en el mercado, las personas son obligadas a promocionarse como material atractivo...se convierten a sí mismas en productos de mercado.»*

Es decir, el desarrollo social en la era de la tecnología hace o debe hacer partícipes a los ciudadanos y adecuarse a cómo entienden éstos el tratamiento de sus datos/privacidad puesto que las evoluciones y circunstancias culturales *(«cultural awareness»*) exigen un esfuerzo de adaptación permanente a las sociedades en general y de los responsables del tratamiento en particular a la hora de llevar a cabo sus misiones. Con carácter general no será igual la noción sobre su ámbito privado o íntimo de un joven de 18 años en el año 2022 que de una persona de 60, 70 u 80 años.

Todo teniendo en cuenta que, desde este marco de la privacidad o ámbito privado, se deriva el control de las interacciones tecnologías y que tales interacciones son información a manejar y contienen datos de carácter personal (identificadores) que exigirán un determinado examen o incluso cierta restricción de actuaciones e informaciones en función de los espacios en los que se desempeñen nuestras actuaciones o las de terceros.

De la misma forma, Kranzberg[53] en sus famosas leyes de la tecnología señalaba que: *«Se ha de valorar que la tecnología no es ni buen ni mala, pero tampoco es neutral"..."La interacción de la tecnología en la ecología social es tal que los desarrollo tecnológicos tiene frecuentemente consecuencias sociales, humanas y sobre el entorno que van más allá de las finalidades inmediatas de los propios dispositivos y prácticas técnicas.»*

Cuestión que viene a ser refrendada por Virginia Eubanks[54] al afirmar que *«La tecnología es todo menos neutral»,* si bien, dicha autora mantiene la visión de que algoritmos no son inocentes, castigan a los más desfavorecidos y cronifican la pobreza, entendiendo que *el «Gran Hermano de la era digital no vigila a individuos, persigue a grandes grupos sociales.»*

Esta última valoración es algo pesimista, si bien, nos hace reflexionar sobre la importancia y el cariz que toman los desarrollos tecnológico-sociales de nuestra era y las actuaciones que se derivan de dichas acciones relativas al tratamiento de datos personales por las distintas entidades público-privadas.

Sin embargo, estos avances no se detienen en desarrollos meramente tecnológicos, sino que ya se hablan de conceptos hibrídos como el Metaverso[55] que vendría a ser un universo creado en el ciberespacio al que se accede con realidad

[53] KRANZBERG. M. *«Technological Education - Technological Style Vol 6 nº 4»*

[54] https://www.larazon.es/cultura/20211210/iqojc6xs2neqlh2n7o3tqlkj64.html

[55] Vid. https://elpais.com/tecnologia/2021-07-29/el-metaverso-la-nueva-frontera-de-las-grandes-tecnologicas.html

virtual y en el que, idealmente, se deberá poder viajar a través de diferentes experiencias de forma compartida con otros millones de usuarios: reuniones de trabajo, oficinas virtuales, conciertos, juegos, tiendas o plazas públicas donde encontrarse con sus amigos o en palabras de Mark Zuckerberg: *«...un entorno persistente y sincrónico en el que podemos estar juntos, que creo que probablemente se parecerá a una especie de híbrido entre las plataformas sociales que vemos hoy en día, pero en un entorno en el que te verás inmerso.»*

Metaversos que no serán únicos y que generarán todo tipo de «problemática» para la realidad social y las personas. Uno de los fundadores de los sistemas de realidad aumentada, Louis Rosenberg, ha señalado que la interactuación en el mundo digital podría *«alterar nuestro sentido de la realidad» y distorsionar «cómo interpretamos nuestras experiencias diarias directas». «Nuestro entorno se llenará de personas, lugares, objetos y actividades que en realidad no existen y, sin embargo, nos parecerán profundamente auténticos»*[56]. De manera que, se podría entender posible que las personas puedan ser objetos de daños y perjuicios en ese campo también.

Estas cuestiones, aun a modo de hipótesis a futuro, han sido tenidas en cuenta por los legisladores a la hora de definir el contenido del paquete de protección de datos de la UE puesto que en propio el RGPD se prevé que: *«El tratamiento de datos personales debe estar concebido para servir a la humanidad»*[57] y en la Directiva de datos policiales se alude a que: *«(2) Los principios y normas relativos a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales deben, cualquiera que sea su nacionalidad o residencia, respetar sus libertades y derechos fundamentales, en particular el derecho a la protección de los datos personales. La presente Directiva pretende contribuir a la consecución de un espacio de libertad, seguridad y justicia. (3) La rápida evolución tecnológica y la globalización han planteado nuevos retos en el ámbito de la protección de los datos personales. Se ha incrementado de manera significativa la magnitud de la recogida y del intercambio de datos personales. La tecnología permite el tratamiento de los datos personales en una escala sin precedentes para la realización de actividades como la prevención, la investigación, la detección o el enjuiciamiento de infracciones penales o la ejecución de sanciones penales.»*

Analizados estos desarrollos sociales y por los motivos expuestos la DDP (al igual que el RGPD) este nuevo paquete normativo cambia el paradigma de regulaciones anteriores y fija que el riesgo para los derechos debe determinarse basándose en una evaluación objetiva, mediante la cual se determine si las operaciones de tratamiento de datos suponen un alto riesgo para los derechos de los interesados y no para los responsables de tratamiento. Un alto riesgo que podemos definir como un nivel elevado en cuanto a la probabilidad y al grado de perjuicio para los derechos y libertades de los interesados derivados del tratamiento específico de sus datos.

---

[56] https://www.muyinteresante.es/tecnologia/articulo/es-peligroso-el-metaverso-de-facebook-821636623435

[57] RGPD. Considerando 4.

Nivel de riesgo o perjuicio efectivo que debe determinarse en base al contenido de los derechos y libertades analizadas y del contexto en el que se ejerza o desarrolle el ejercicio de esos derechos y libertades.

En este último aspecto incidió el Constitucional en su sentencia STC 27/2020, de 24 de febrero de 2020[58]," que extendía el ejercicio de los derechos al mundo digital como si fuera ejercido en el *«mundo analógico»*:

> *«Es innegable que los cambios tecnológicos cada vez más acelerados que se producen en la sociedad actual afectan al conjunto global de los ciudadanos repercutiendo directamente en sus hábitos y costumbres. También lo es la afectación de los derechos fundamentales al honor, a la intimidad, a la propia imagen y a la protección de datos de carácter personal (art. 18 CE) por el uso masivo de las tecnologías de la información y de la comunicación y de los servicios de redes sociales en Internet. El aumento de popularidad de las redes sociales ha transcurrido en paralelo al incremento de los niveles de intercambio de contenidos a través de la red. De este modo, los usuarios han pasado de una etapa en la que eran considerados meros consumidores de contenidos creados por terceros, a otra –la actual– en la que los contenidos son producidos por ellos mismos. Con plataformas como Facebook, Twitter, Instagram o Tuenti, por citar solo algunas, los usuarios (porque jurídicamente ostentan tal condición) se han convertido en sujetos colaborativos, ciudadanos que interactúan y que ponen en común en redes de confianza lo que tienen, lo que saben o lo que hacen, y que comparten con un grupo más o menos numeroso de destinatarios –usuarios igualmente de la redes sociales en Internet– todo tipo de imágenes, información, datos y opiniones, ya sean propios o ajenos. La amplitud de actividades que pueden desplegarse a través de unas redes sociales en Internet gracias a las prestaciones de la Web 2.0, facilitan la actividad colaborativa del usuario en la gestión, elaboración y publicación de contenidos, de modo que en pocas décadas ha pasado de ser un sujeto pasivo receptor de información a un sujeto activo que elabora, modifica, almacena y comparte información. Piénsese, por ejemplo, que según los datos que ofrece la propia red social Facebook, en el mundo hay más de 1.860 millones de usuarios activos y cada día acceden solo a esta red social más de 1.150 millones de personas. Se suben más de 300 millones de fotografías diarias y, en un minuto se publican más de 510.000 comentarios, se actualizan más de 293.000 estados y se suben más de 136.000 fotografías.*
>
> *En este contexto es innegable que algunos contornos de los derechos fundamentales al honor, a la intimidad y a la propia imagen (art. 18 CE), garantes todos ellos de la vida privada de los ciudadanos, pueden quedar desdibujados y que la utilización masificada de estas tecnologías de la información y de la comunicación, unida a los cambios en los usos sociales que ellas mismas han suscitado, añaden nuevos problemas jurídicos a los ya tradicionales. Si bien es un hecho que el funcionamiento de las redes sociales en Internet permite la difusión de información personal, también lo es que puede significar una pérdida de control de la información suministrada por el propio usuario.*

[58] Sala Segunda. Sentencia 27/2020, de 24 de febrero de 2020. Recurso de amparo 1369-2017. ECLI:ES:TC:2020:27

Un ejemplo de ello lo encontramos en las fotografías que se divulgan y en las etiquetas que permiten individualizar a una persona, en los comentarios y opiniones, y en la información que sobre un determinado sujeto se coloca en los perfiles y en los distintos espacios de acceso público. Es usual encontrarse que, en numerosos casos, los usuarios publican en la red social en Internet no solo información sobre sí mismos, sino también de otras personas (usuarios o no) y que lo más habitual es que no hayan recabado su autorización, antes o después de hacerlo. Igualmente hay que reparar en que cuando se toma una fotografía o se graba un videoclip, no solo se está creando una imagen, sino que esta incluye datos (metadatos) sobre quién ha hecho, dónde se ha hecho o incluso qué dispositivo se ha utilizado, los cuales pueden ser conocidos por cualquiera que tenga acceso a ella.

Contemplado de esta manera el panorama tecnológico actual y aceptando que la aparición de las redes sociales ha cambiado el modo en el que las personas se socializan, hemos de advertir sin embargo –por obvio que ello resulte– que los usuarios continúan siendo titulares de derechos fundamentales y que su contenido continúa siendo el mismo que en la era analógica. Por consiguiente, salvo excepciones tasadas, por más que los ciudadanos compartan voluntariamente en la red datos de carácter personal, continúan poseyendo su esfera privada que debe permanecer al margen de los millones de usuarios de las redes sociales en Internet, siempre que no hayan prestado su consentimiento de una manera inequívoca para ser observados o para que se utilice y publique su imagen... (...)....

Pero el hecho de que circulen datos privados por las redes sociales en Internet no significa de manera más absoluta –como parece defender la demandante de amparo– que lo privado se haya tornado público, puesto que el entorno digital no es equiparable al concepto de «lugar público» del que habla la Ley Orgánica 1/1982, ni puede afirmarse que los ciudadanos de la sociedad digital hayan perdido o renunciado a los derechos protegidos en el art. 18 CE. Los particulares que se comunican a través de un entorno digital y que se benefician de las posibilidades que ofrece la Web 2.0 no pueden ver sacrificados por este solo hecho los derechos fundamentales cuya razón de ser última es la protección de la dignidad de la persona. Aunque los riesgos de intromisión hayan aumentado exponencialmente con el uso masivo de las redes sociales, para ahuyentarlos debemos seguir partiendo del mismo principio básico que rige el entorno analógico y afirmar que el reconocimiento constitucional de los derechos fundamentales comprendidos en el art. 18 CE conlleva la potestad de la persona de controlar los datos que circulan en la red social y que le conciernen. Por consiguiente, reiteramos que, salvo que concurra una autorización inequívoca para la captación, reproducción o publicación de la imagen por parte de su titular, la injerencia en el derecho fundamental a la propia imagen debe necesariamente estar justificada por el interés público preponderante en tener acceso a ella y en divulgarla.»

Observadas las distintas definiciones y afirmaciones expuestas, derivado de la interpretación del TC, se pueden enmarcar muy breve y concisamente los límites de los derechos siguientes:

Derecho a la autodeterminación informativa o *«Habeas Data»*: Poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un partic-

ular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso.

El Derecho a la Intimidad: Aquel que tiene por finalidad proteger respecto de las personas *«un ámbito reservado de su vida, vinculado con el respeto de su dignidad como persona, frente a la acción y el conocimiento de los demás, sean estos poderes públicos o simples particulares. De suerte que el derecho a la intimidad atribuye a su titular el poder de resguardar ese ámbito reservado, no solo personal sino también familiar, frente a la divulgación del mismo por terceros y una publicidad no querida. No garantiza una intimidad determinada sino el derecho a poseerla, disponiendo a este fin de un poder jurídico sobre la publicidad de la información relativa al círculo reservado de su persona y familia, que se desea mantener al abrigo del conocimiento público. Lo que el artículo 18.1 de la CE garantiza, es, pues, el secreto sobre nuestra propia esfera de vida personal y, por tanto, veda que sean los terceros, particulares o poderes públicos, quienes decidan cuales son los contornos de nuestra vida privada»*.

El Derecho a la Propia Imagen, éste está dirigido a *«proteger la dimensión moral de las personas, que atribuye a su titular un derecho a determinar la información gráfica generada por sus rasgos físicos personales que puede tener difusión pública. La facultad otorgada por este derecho, en tanto que derecho fundamental, consiste en esencia en impedir la obtención, reproducción o publicación de la propia imagen por parte de un tercero no autorizado, sea cualquiera su finalidad –informativa científica, cultural, comercial– perseguida por quien la capta o difunde; pero no puede deducirse que el derecho a la propia imagen, en cuanto límite al obrar ajeno, comprenda el derecho incondicionado y sin reservas de impedir que los rasgos físicos que identifican a la persona se capten o se difundan, pues como cualquier otro derecho, no es un derecho absoluto, y por ello su contenido se encuentra delimitado por el de otros derechos y bienes constitucionales».*

El Derecho al Honor: Aunque Calderón de la Barca aludía a este concepto en su famosa obra «El Alcalde de Zalamea» exponiendo que: *«Al rey la hacienda y la vida se ha de dar, pero el honor es patrimonio del alma y el alma sólo es de Dios...»*[59], ni la CE ni la Ley Orgánica 1/1982, de 5 de mayo, ofrecen un concepto o extensión específicos del honor, el Tribunal Constitucional, lo ha calificado como concepto jurídico indeterminado. Ha sido, pues, tarea de la doctrina jurídica y de la jurisprudencia delimitar y clarificar en la medida de lo posible el confuso concepto de honor, a pesar de la dificultad de acometer esta tarea considerando la relatividad y circunstancialidad del mismo, puesto que es un concepto *«dependiente de las normas, valores e ideas sociales vigentes en cada momento.»*

Porque es imprescindible tener todos estos derechos en consideración en conjunto y en relación con otros como el derecho a recibir una información veraz o el derecho a la libertad de expresión, pues porque tener claros los conceptos y su extensión nos evitará incurrir en distintas responsabilidades como actores en su manejo o ejercicio.

[59] CALDERÓN DE LA BARCA, P. *«El Alcalde de Zalamea»*. Ed. Anaya. ISBN 978-8467840094

Veamos un reciente ejemplo contenido en una resolución a un expediente sancionador de la AEPD (PS/00493/2020), donde se sanciona con 6000 euros a un club deportivo por publicar en una red social y en su página web una sentencia contra uno de sus socios por una serie de regularidades cometidas en la persona jurídica y en la que constan sus datos personales y en donde se ven afectados el derecho a a la intimidad y el derecho a la protección de datos.

La Agencia entiende que el derecho a la protección de datos puede colisionar con el de la libertad informativa, sin embargo, la relevancia del cargo del reclamante no es de carácter público ni se trata de un asunto penal (únicamente disciplinario), por lo que no se cumpliría la proporcionalidad en el tratamiento para la finalidad de informar a los socios y no se contemplan los derechos afectados del sancionado, por lo que no puede acogerse la prevalencia del interés legítimo en la exposición en abierto de la sentencia íntegra en formato .pdf y su consulta posible en el motor de búsqueda.

El quid de la cuestión sería el derivado de que, aunque las actuaciones judiciales sean públicas, no se justifica que los datos personales que contienen sean revelados en un ámbito distinto al proceso judicial y que se expongan además de una forma completa fuera del ámbito en el que propiamente es el afectado y concernido por las actuaciones, no siendo la sentencia definitiva, estando, pendiente de recurso.

No prevaleciendo por lo tanto el derecho a conocer el contenido íntegro de la resolución judicial por cualquier persona sobre el derecho del afectado a su intimidad y, del mismo modo, a su derecho a la protección de datos, dados los amplios términos en que se produce la difusión no siendo necesarios en su totalidad cuando afecta a los intereses y gestiones, únicamente, de los asociados.

III. CONCEPTOS BÁSICOS

Se ha referido previamente a la necesidad de conocer lo mejor posible la extensión y el significado de los conceptos que se manejan en el marco de la protección de datos de carácter personal. Una vez fijada la extensión y contenido básico del derecho, es necesario conocer cuáles serían los elementos formales y materiales de los conceptos contenido en las normas que lo regulan.

Esto es importante para poder desarrollar las distintas actuaciones de la manera más eficaz y eficiente posible, de modo que tanto los responsables del tratamiento como las personas que dependen o quedan bajo el sistema orgánico o funcional de los mismos, puedan desempeñar sus misiones de forma que en todo momento quede garantizada la protección del derecho a la protección de datos personales.

¿Qué es un dato? ¿Qué es la información? ¿Qué es un dato de carácter personal? Estas y otras preguntas resultan recurrentes entre las personas que se acercan por primera vez a esta materia, por lo que como actuación básica e ineludible deberían intentar discernir cuál es el significado y la extensión de estas definiciones.

Según el Diccionario de la lengua española la RAE (DRAE) los datos serían la información sobre algo concreto que permite su conocimiento exacto o sirve para deducir las consecuencias derivadas de un hecho (información necesaria para el conocer algo) o la información dispuesta de manera adecuada para su tratamiento por una computadora.

La información (*Del lat. informatio, -ōnis 'concepto', 'explicación de una palabra»*), entre otras acepciones, la define como: *«3. f. Averiguación jurídica y legal de un hecho o delito. 5. f. Comunicación o adquisición de conocimientos que permiten ampliar o precisar los que se poseen sobre una materia determinada. 6. f. Conocimientos comunicados o adquiridos mediante una información."*

Esta definición de información, obviamente tiene otras muchas acepciones y su uso (obtención de la información) por parte de las autoridades competentes a los fines prevenidos se puede afirmar que es una de las misiones básicas recogidas en el artículo 11 de la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad y, por lo tanto, éstas están obligadas y legitimadas a captar, recibir y analizar cuantos datos tengan interés para el orden y la seguridad pública, y estudiar, planificar y ejecutar los métodos y técnicas de prevención de la delincuencia.

Incidiendo en estas ideas, del mismo modo, el Diccionario panhispánico del español jurídico (en adelante DEJ), define dato como la información necesaria para el conocimiento de algo y la información, con carácter general, como la averiguación, indagación, comunicación y puesta en conocimiento de algo.

La información y el conocimiento a lo largo de la historia siempre han sido una fuente de fuerza y de poder, no obstante, en las sociedades democráticas, el tratamiento y el derecho a la información se protegen como derechos fundamentales de todas las personas.

Para poder realizar sus funciones de investigación o prevención del delito, en el caso de los cuerpos policiales, ninguna de estas organizaciones puede carecer de bases de información y ficheros de tratamiento ya sean manuales o informatizados.

Además de su uso, éstos están obligados y legitimados a captar, recibir y analizar cuantos datos tengan interés con la finalidad proteger los derechos e ga-

rantizar el orden y la seguridad pública, así como para estudiar, planificar y ejecutar métodos y técnicas de prevención de la delincuencia.

Pero esta captación y tratamiento de la información debe realizarse siempre conforme a la legalidad establecida, puesto que en caso contrario se incurrirían en ilícitos penales y, además, los datos e informaciones aportados a los procedimientos o procesos carecerían de validez, lo que haría tirar por tierra las investigaciones o misiones realizadas.

Tradicionalmente las principales funciones que cumple la información y la obtención de datos personales que puede llevar aparejada pueden resumirse en cuatro grandes funciones: *«Prevención, Detección, Punitiva o Conocimiento»*.

Prevención: Función principal de toda información, supone prever o descubrir las actividades que originen peligros para la seguridad ciudadana o supongan una agresión a la seguridad del Estado y tomar las oportunas medidas antes de que aquellas se produzcan.

Detección: Función que consiste en detectar con la premura necesaria las amenazas a los derechos y la seguridad para poder responder de la manera y en el tiempo adecuados (tiempos de respuesta, «modus operandi», etc.)

Punitiva: Partiendo de que la seguridad total no existe, cuando se produce el delito, la información permite adoptar las medidas necesarias para identificar a los autores de los hechos delictivos y ponerlos ante la autoridad judicial competente.

Conocimiento: Esta finalidad es la denominada inteligencia, que consistiría en trasladar información a la autoridad competente para que pueda adoptar las decisiones políticas o de seguridad más adecuadas.

Como se apuntaba la información que se trate, debe hacerse conforme a los presupuesto legales oportunos, por lo que la transparencia (que no se debe confundir con publicidad o acceso indiscriminado) en estos ciclos es fundamental para asentar las bases de las sociedades democráticas.

No se trata de hacer público cómo y qué información se recoge, si bien, debe quedar trazado todo el procedimiento y la información o los datos recogidos debe estar siempre en condiciones de ser presentada ante la autoridad judicial o la que resulte competente. En caso contrario, como se apuntaba, no sería válida ni útil para los procedimientos, puesto que la base de las actuaciones quedaría deslegitimada y contaminada.

Para que la información sea legítima se debe cumplir lo siguiente:

- Los medios de obtención de la información son lícitos, es decir, que están amparados en la Ley.
- Se limite a la finalidad legal de tratamiento.
- Las actividades están supervisadas y sometidas a control por autoridades independientes.

Del mismo modo, no debemos confundir información con inteligencia puesto que, dentro de nuestro ámbito, cuando hablamos de ésta nos referimos o al proceso el cual elaboramos la información, dejándola lista para ser utilizada, es decir, el proceso que permite interpretar la información y darle significado, permitién-

donos conocer y predecir hechos hostiles, disminuir las incertidumbres y coadyuvar a la toma de decisiones o a las unidades o departamentos que recopilan o tratan dicha información.

La inteligencia puede ser principalmente táctica u operativa que se conformaría con las informaciones relacionadas entre sí que tienen valor por sí misma, para uso inmediato y que permite resultados a corto o medio plazo o estratégica, cuya definición sería el conjunto de informaciones que proporcionan un conocimiento global sobre una amenaza, y permite anticipar la comisión delictiva (función preventiva). Pueden ser predicciones analíticas y prospectivas a medio y largo plazo.

La recopilación de información lleva un procedimiento que suele denominarse ciclo de la información y éste es diferente en cada organización, pero con carácter general se suele dividir en las siguientes fases: Obtención, Evaluación, Tratamiento, Análisis y Difusión.

Desde el punto de vista de las finalidades de prevención, detección o investigación de delitos, fuente de información sería todo aquel elemento (*cosa, persona o actividad*) que es capaz de generar información relevante para las misiones de averiguación del delito, descubrimiento y aseguramiento del delincuente y la de captación de información encomendadas a los cuerpos policiales. Estas fuentes son de origen y cualidades muy distintas, pero se pueden agrupar en tres grandes grupos: por su dependencia (*propias o ajenas*), por su origen (*documentales, técnicas o humanas)* o por su grado de accesibilidad (*abiertas o públicas, semipúblicas o clasificadas o restringidas)*

Analizados estos conceptos generales, la normativa sobre protección de datos personales precisa el significado de dato de carácter personal como toda información sobre una persona física identificada o identificable; considerándose persona física identificable aquellas 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.

Esto lo recoge el DEJ de la siguiente forma:

Dato de carácter personal: *«Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de otro tipo concerniente a personas físicas identificadas o identificables.»*

Persona física o natural: (Art. 29 sgts Código Civil) La personalidad se adquiere en el momento del nacimiento con vida, una vez producido el entero desprendimiento del seno materno.

Persona identificada: Persona que sea distinguible de todas las demás personas y reconocible como individuo[60].

Perdona física identificable: *«Persona cuya identidad pueda determinarse directa o indirectamente mediante uno o varios elementos específicos característicos de su identidad física, fisiológica, psíquica, económica, cultural o social.»* En este supuesto

[60] Curso: *«Data Protection and Privacy Rights»*, del Consejo de Europa. http://help.elearning.ext.coe.int

es oportuno recordar que la protección otorgada por la normativa debe aplicarse a éstas independientemente de su nacionalidad o lugar de residencia, en lo que se refiere al tratamiento de sus datos personales (carácter de universalidad)

Para considerar si una persona resulta identificable principalmente debemos acudir al contenido del considerando nº 26 del RGPD que dispone que para determinar si una persona es identificable o no, se deben tener en cuenta todos los medios razonablemente susceptibles de ser utilizados, como el control individual, ya sea por parte de los responsables o de terceros. La determinación de si son o no datos personales a menudo requerirá un análisis individualizado de cada caso.

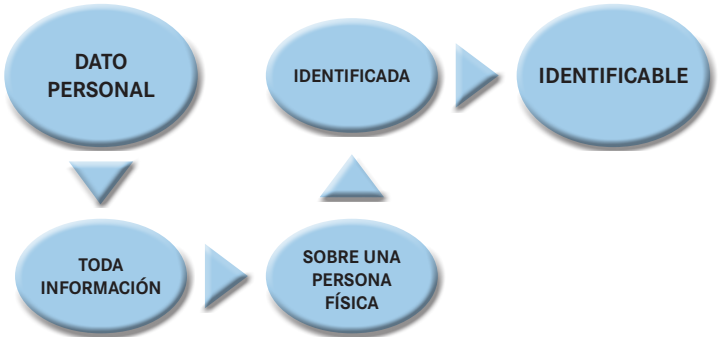
De igual modo, no se considerará identificable si su identificación requiere un tiempo, esfuerzos o recursos irrazonables. Estos factores deben considerarse tomando como referencias el tipo de tratamiento, el costo, los beneficios de la identificación, los responsables que lo llevan a cabo y la tecnología utilizada.

Identificación directa: la atribuible a la persona en relación con su identificador.

Identificación indirecta: Según la AEPD, sería aquella que puede tener lugar como consecuencia de información de una o varias fuentes que por sí misma o en combinación de otros factores puede permitir la re-identificación de las personas cuando sus datos sean anónimos (no conocidos) o hubieran sido anonimizados (y por derivación aquellos que en principio no puedan ser considerados datos personales). Por ejemplo, la combinación de sexo, edad, lugar de nacimiento y padecimiento de una determinada enfermedad pueden permitir la identificación indirecta de una persona concreta si analizamos la información en su conjunto de manera que pueda deducirse o inferirse su identidad.

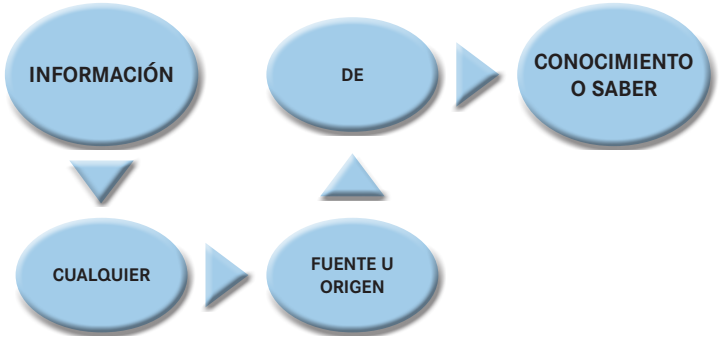
Sin perjuicio de existir otras definiciones más o menos técnicas y otros ejemplos, en base a lo apuntado previamente, los conceptos básicos podrían quedar encuadrados en estos gráficos:

Para hablar de dato personal[61]:



[61] FERNÁNDEZ GONZÁLEZ. C, AYLLÓN SANTIAGO, H. Prólogo: Jorge Álvaro Navas Elorza *«Tratamiento de datos de carácter personal en el ámbito policial» ISBN:978-84-290-2433-3 Editorial Reus. 1ª Edición.*

De Información:

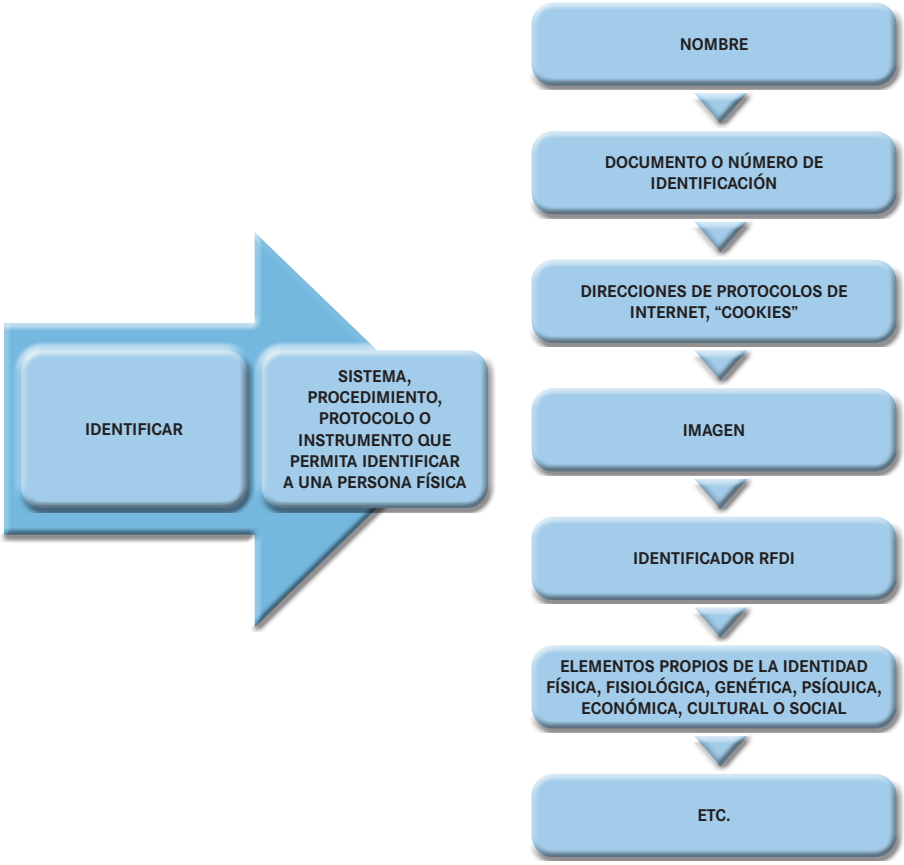


Persona física identificada o identificable:

El considerando 21 de la DDP, recoge que los principios de la protección de datos deben aplicarse a toda la información relativa a una persona física identificada o identificable. Como hemos visto, para determinar si una persona física es identificable deben tenerse en cuenta todos los medios con respecto a los cuales existe una probabilidad razonable de que puedan ser utilizados por el responsable del tratamiento o por cualquier otra persona para la identificación directa o indirecta de la misma. Para determinar si existe una probabilidad razonable de que se utilicen unos medios determinados para la identificación deben tenerse en cuenta todos los factores objetivos, como los costes y el tiempo necesarios para la identificación, valorando igualmente tanto la tecnología disponible en el momento del tratamiento como los avances tecnológicos.

Por tanto, se puede afirmar en sentido contrario que los principios de protección de datos personales no deben aplicarse a la información anónima, a saber, información que no guarda relación con una persona física identificada o identificable, ni a los datos personales convertidos en anónimos de forma que el interesado al que se refieren ya no resulte identificable en modo alguno.

Identificador:



Estos identificadores pueden ser cualquier información o elemento que permita identificar a una persona física. Por ejemplo, en una operación reciente de INTERPOL[62] se procedió a identificar a una persona por un tatuaje observado en un video (que previamente tendrían que relacionar de algún modo con esta persona) lo que convierte a ese elemento (tatuaje) en un dato personal y obliga a que

[62] Arrested in the Dominican Republic and extradited to Italy: 'Ndrangheta fugitive Marc Feren Claude Biart, wanted on drug trafficking charges since 2014, lands in Italy to face justice. Authorities located him after recognising his tattoos in a YouTube video. https://www.linkedin.com/posts/interpol_ndrangheta-arrest-in-dominican-republic-activity-6782612139204050944-rKhL/

el organismo actuante cumpla con los presupuestos oportunos para no vulnerar sus derechos en cuanto a la normativa de protección de datos.

Dato no personal: Dato que no identifique a una persona física o no facilite elementos suficientes para determinar dicha identidad y que no derive en una probabilidad razonable de identificarla utilizando cualquier medio. Para determinar dichos medios habrán de tenerse en cuenta todos los factores objetivos, como los costes, el tiempo, la tecnología disponible o los avances tecnológicos[63].

Dato personal compuesto: Según Polo Roca[64],*…" será aquel que está compuesto por varios «datos no personales» (ya que no identifican ni permiten identificar a una persona física), pero que al considerarlos en su conjunto conforman un dato personal."*

Esta definición deriva de la STJUE (Gran Sala) de 8 de abril de 2014, asuntos acumulados C-293/12 y C-594/12, Digital Rights Ireland y Seitlinger y otros, en la que el Tribunal implantó una doctrina que se ha mantenido en todos los procesos posteriores: *«Estos datos [datos de comunicaciones electrónicas], considerados en su conjunto, pueden permitir extraer conclusiones muy precisas sobre la vida privada de las personas cuyos datos se han conservado, como los hábitos de la vida cotidiana, los lugares de residencia permanentes o temporales, los desplazamientos diarios u otros, las actividades realizadas, sus relaciones sociales y los círculos sociales que frecuentan.»*

Dato estructurado: También denominados datos cuantitativos, son datos que han sido formateados e incorporados en un modelo de datos definido. Son los datos con los que se suele trabajar (texto en filas y columnas con etiquetas, bases de datos, hojas de cálculo, etc.)

Dato no estructurado: Denominados asimismo como datos cualitativos, serían aquellos que se presentan de forma absoluta sin procesar en modo alguno. Su naturaleza es categórica y característica, presentándose en forma de datos binarios no comprensibles en un principio para el lenguaje humano.

Dato sintético: aquel que es creado de manera artificial de ser derivado de una persona real, sirviendo como alternativa a los datos personales para una infinidad de actuaciones. Estos datos pueden conservar las características de un conjunto de datos personales previo, pero generan un conjunto de datos artificiales que no permiten inferir o averiguar los datos originales. Los datos sintéticos suelen ser creados por Inteligencia Artificial (*«machine learning»*) adiestrada sobre los datos reales.

A partir de estos elementos básicos, otras definiciones de importancia que se deben manejar serían las siguientes:

Tratamiento: Cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos

[63] Considerando 26 del RGPD.

[64] POLO ROCA, A. «Datos, datos, datos: el dato personal, el dato no personal, el dato personal compuesto, la anonimización, la pertenencia del dato y otras cuestiones sobre datos.» Universidad de Deusto. ISSN 0423-4847 • ISSN-e 2386-9062, Vol. 69/1, enero-junio 2021, págs. 211-240 http://www.revista-estudios.deusto.es/

automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión, o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.

De esta definición se derivan cuestiones importantes que han generado cierta confusión, como, por ejemplo, que la posibilidad de la mera consulta de datos de un fichero se convierta en una actividad de tratamiento y, por lo tanto, las entidades deben tenerla (como al resto de actividades) recogida, archivada y publicitada formalmente. *«Tratamiento XXX, sobre consultas al fichero XXXXX».* Esta cuestión carece de toda duda, puesto que el simple acceso a los datos está dentro de la definición y por lo tanto tiene que estar documentado y legalizado en todos sus extremos.

Este concepto también es aplicable a las actividades que se realicen entre entidades en más de un Estado miembro de un responsable o encargado del tratamiento en la Unión, si el responsable o el posible encargado está establecido en más de un Estado miembro y también incluiría las actividades de una autoridad responsable que pueda afectar sustancialmente a interesados en más de un Estado miembro.

La forma en la que estos datos sean conservados o tratados no es determinante para aplicar la normativa de protección de datos ya que las comunicaciones escritas, verbales, digitales o biométricas pueden contener datos que identifiquen a una persona. Del mismo modo, los datos personales incluyen aquella información relacionada con aspectos privados de la persona, sus actividades profesionales y su vida pública. Estas afirmaciones han venido recogidas tanto en sentencias del TEDH[65] como en el TJUE.[6667]

Fichero: Todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica.

Se recuerda de nuevo que la LOPDP 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. Por lo que, en este caso de tratamientos no automatizados, los ficheros o conjuntos de ficheros, así como sus portadas, que no estén estructurados con arreglo a criterios específicos, no deberían entrar en su ámbito de aplicación (ni en el del RGPD)

Categorías especiales de datos[68]: son aquellos datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filo-

[65] Asuntos Amann c. Suiza y Niemietz c Alemania.

[66] Volker y Markus Schecke y Harmunt Eifert c. Land Hessen.

[67] Curso Data Protection and Privacy Rights del Consejo de Europa. http://help.elearning.ext.coe.int

[68] Considerando 37 de la Directiva de datos policiales: *«Especial protección merecen los datos personales que, por su naturaleza, son particularmente sensibles en relación con los derechos y las libertades fundamentales, ya que el contexto de su tratamiento puede generar riesgos importantes para los derechos y las libertades fundamentales. Dichos datos personales deben incluir aquellos que pongan de manifiesto el origen racial o étnico, entendiéndose que el término "origen racial" empleado en la presente Directiva no implica la aceptación por parte de la Unión Europea de teorías que traten de determinar la existencia de razas humanas diferentes. Tales datos personales no*

sóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física.

Estos son lo que con la normativa anterior se denominaban *«datos especialmente protegidos»* y su tratamiento se debe efectuar conforme al artículo 9 del RGPD y al artículo 13 de la LOPDP.

En consonancia con el RGPD el tratamiento de estos datos estaría prohibido salvo que concurran determinadas circunstancias y faculta a los Estados para mantener o introducir condiciones adicionales, inclusive limitaciones, con respecto al tratamiento de algunos de éstos como serían los datos genéticos, datos biométricos o datos relativos a la salud que posteriormente se detallan.

Sin embargo, en base a la Directiva y su «desarrollo» en el aludido artículo 13, el tratamiento no está prohibido y se permite cuando sea estrictamente necesario, con sujeción a las salvaguardias adecuadas para los derechos y libertades del interesado y únicamente cuando:

- Lo autorice una disposición legal.
- aunque no haya tal previsión legal, cuando exista la necesidad de proteger los intereses vitales del interesado (concepto jurídico indeterminado que deberá concretarse en el tráfico jurídico y en la práctica diaria);
- cuando los datos personales se hayan hecho manifiestamente públicos por el interesado.

Veamos un supuesto; como vemos, la propia naturaleza de un tratamiento de datos personales especialmente sensibles, constituye una injerencia en la esfera jurídica de una persona física, es decir, un menoscabo de su integridad, de conformidad con el artículo 3 de la Carta. Por lo tanto, la toma de la huella dactilar y de la obtención de muestras de ADN a priori podría parecer contraria al artículo 3 de la Carta.

Pero esto no es así, el derecho a la protección de los datos personales está recogido en el artículo 8 de la Carta. Estos derechos, consagrados en los artículos 3 y 8 de la Carta, pueden limitarse únicamente en las condiciones establecidas en

---

deben ser objeto de tratamiento, salvo que el tratamiento esté supeditado a las garantías adecuadas de protección de los derechos y libertades del interesado que se establecen en la legislación y esté permitido en los casos autorizados por la ley; o, si no está ya autorizado por dicha legislación, que el tratamiento sea necesario para proteger los intereses vitales del interesado o de otra persona, o que el tratamiento se refiera a datos que el interesado ya ha hecho públicos de forma manifiesta. Entre las garantías adecuadas de protección de los derechos y libertades del interesado pueden figurar, por ejemplo, la posibilidad de recopilar tales datos únicamente en relación con otros datos de la persona física afectada, la posibilidad de proteger adecuadamente los datos recopilados, el establecimiento de normas más estrictas para el acceso a los datos por parte del personal de la autoridad competente, o la prohibición de transmisión de dichos datos. El tratamiento de este tipo de datos también debe estar jurídicamente permitido si el interesado ha acordado de forma explícita que el tratamiento de los datos resulte especialmente intrusivo para las personas. Sin embargo, el consentimiento del interesado no debe constituir en sí mismo un fundamento jurídico para que las autoridades competentes procedan al tratamiento de datos personales sensibles como los mencionados.»

su artículo 52 (considerando 104 de la DDP) siempre que se cumplan los citados requisitos.

En consecuencia, tanto el artículo 10, letra a), de la Directiva 2016/680 como el artículo 52 de la Carta imponen como la principal exigencia de que la recogida de datos biométricos y genéticos debe estar establecida por la ley.

La LOPDP, viene a dar carta de naturaleza a esta obligación y en el apartado 2 de su artículo 13, dispone con carácter general que:

> *«2. Las autoridades competentes, en el marco de sus respectivas funciones y competencias, podrán tratar datos biométricos dirigidos a identificar de manera unívoca a una persona física con los fines de prevención, investigación, detección de infracciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública.»*

Por lo tanto, el resumen podría ser el siguiente:

COMPETENCIA+ NECESIDAD + GARANTIAS + SUPUESTOS (LEY, INTERESES VITALES, MANIFIESTAMENTE PÚBLICOS) + ¿ÉTICA?

Naturalmente, las autoridades competentes tienen que tener capacidad legal para la finalidad perseguida (*Vid. artículo 8 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público*)[69], esto es, que después valorar caso a caso la necesidad de tratar los datos a través de la observancia del principio de proporcionalidad: la medida sea susceptible de conseguir el objetivo propuesto (juicio de idoneidad); que la actuación resulte necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y que la misma sea ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto).

Para el estudio de este concepto resultan especialmente relevantes las *«Directrices del SEPD para la evaluación de la proporcionalidad de las medidas que limitan los derechos fundamentales a la intimidad y a la protección de los datos personales»* donde se expone en primer lugar que la necesidad es una condición previa

[69] *«Artículo 8. Competencia. 1. La competencia es irrenunciable y se ejercerá por los órganos administrativos que la tengan atribuida como propia, salvo los casos de delegación o avocación, cuando se efectúen en los términos previstos en ésta u otras leyes. La delegación de competencias, las encomiendas de gestión, la delegación de firma y la suplencia no suponen alteración de la titularidad de la competencia, aunque sí de los elementos determinantes de su ejercicio que en cada caso se prevén. 2. La titularidad y el ejercicio de las competencias atribuidas a los órganos administrativos podrán ser desconcentradas en otros jerárquicamente dependientes de aquéllos en los términos y con los requisitos que prevean las propias normas de atribución de competencias. 3. Si alguna disposición atribuye la competencia a una Administración, sin especificar el órgano que debe ejercerla, se entenderá que la facultad de instruir y resolver los expedientes corresponde a los órganos inferiores competentes por razón de la materia y del territorio. Si existiera más de un órgano inferior competente por razón de materia y territorio, la facultad para instruir y resolver los expedientes corresponderá al superior jerárquico común de estos.»*

a la proporcionalidad y esta medida vendría derivada de que el derecho a la protección de datos no es un derecho absoluto y puede limitarse, siempre que las limitaciones cumplan los requisitos previstos en el artículo 52, apartado 1, de la Carta de los Derechos fundamentales de la Unión.

Superada esta fase, se debe evaluar si se ajusta a uno de los supuestos apuntados y, de ser así, implementar las garantías necesarias en función de nivel de riesgo para el derecho de los interesados.

Estos supuestos son complementarios, esto es, el segundo y el tercer supuesto, aunque se puedan realizar, también deben ser conformes a la legalidad vigente y a la ética presumible a las autoridades (ej. aunque una persona hiciera manifiestamente pública su orientación sexual o religión, ¿pueden existir ficheros que traten inmotivadamente dicha circunstancia? La respuesta debe ser en todo caso negativa) ¿Se pueden tratar motivadamente cumpliendo los requisitos? En este caso parece clara la posibilidad de una respuesta afirmativa, pero después de haber valorado todos los requerimientos apuntados, como por ejemplo en la investigación de delitos de odio contra personas de colectivos atacados por su identidad o condición sexual, para realizar un informe sobre las necesidades especiales (INA) de estas víctimas, etc.

Otra cuestión de relevancia, dada la incidencia operacional a día de hoy, resultaría de concretar lo que se conoce por hacer una cuestión manifiestamente pública a la hora de posibilitar en este campo el uso de informaciones derivadas de fuentes abiertas, como por ejemplo fuentes públicas de Internet o de la exhibición pública (fuera del ámbito privado o íntimo) de elementos, símbolos o ropas que pudieran ser identificadores. En estos supuestos, por ejemplo, no será igual obtener la información de un medio de comunicación que de una aplicación como una red social, un diario, fuentes oficiales o de la obtención de datos en la vía pública. En los primeros casos, las distintas políticas de uso de las aplicaciones o sistemas de los que se pretenden obtener las imágenes, en base a las condiciones para la posible cesión de los contenidos que se almacenen en las mismas a las autoridades competentes con fines de investigación, la forma en la que se accede a dichas imágenes del repositorio electrónico, la posibilidad de que las aplicaciones cuenten con sistemas de ofuscación de datos y otras consideraciones, marcaran su definición y forma de uso.

Es decir, dada las distintas finalidades de tratamiento, el uso de las denominadas técnicas o herramientas OSINT (*Open Source Intelligence, en español Inteligencia de Fuentes Abiertas*), podrá ser incluido o no en los procesos de las entidades o personas que lo utilizan en virtud del propósito de dichas actuaciones teniendo siempre en cuenta la interpretación que hacen las autoridades competentes.

En el tercer supuesto citado (*por lo que respecta específicamente a los tratamientos del RGPD)* se debe tener en cuenta el contenido del dictamen N/REF: 0089/2020 del Gabinete Jurídico de la de la AEPD, donde al hablar sobre listas negras o blancas de interesados dejaba clara la imposibilidad de acudir a *«fuentes accesibles al público»* con carácter general para realizar tratamientos basados en la legitimación por *«interés legítimo»* sin que en estos casos se supere el juicio de ponderación oportuno de forma que no se vulneren los derechos y libertades de los interesados. En su página 62 señala:

> *«En el RGPD, para la existencia del interés legítimo como base jurídica del tratamiento, no se requiere (i) que los datos figuren en fuentes accesibles al público, (ii) ni tampoco se establece para la legitimidad de dicha causa el que "no se vulneren" los derechos y libertades fundamentales del interesado, sino que se habrá de realizar una ponderación para determinar la prevalencia entre el interés legítimo alegado y los "intereses, o los derechos y libertades fundamentales" del interesado que requieran la protección de datos personales (art. 6.1 f) RGPD).»*

Si se analizan estas conclusiones que contiene, creemos que se nos facilita una imagen clara de la intención de la Autoridad de Control en estos supuestos, por lo que sería de mucho interés leer este documento.

De hecho, varias autoridades de control de la Unión han sancionado con multas importantísimas a varias empresas por obtener datos personales de *«fuentes de acceso público»* por distintas finalidades (como la capacidad crediticia, obtención de datos biométricos de imágenes, etc.) al entender que la finalidad no era compatible con el tratamiento originario (la publicación o publicidad)

Por otro lado, con respecto a este tipo de datos, otra cuestión a valorar sería que desde un punto de vista del Derecho Penal, la definición de *«categoría especiales de datos personales»* está siendo interpretada de manera un tanto diferente *(para aplicar principalmente el artículo 197 del C.P)*, como observamos en la STS 1383/2019[70], que señala en su apartado TERCERO, punto 3:

> *«...(...)...sobre los datos personales. En este sentido, señalábamos en la sentencia núm. 586/2016, que el bien jurídico objeto de protección no es la intimidad, entendida en el sentido que proclama el artículo 18.1 de la Constitución Española, sino la autodeterminación informativa a que se refiere el artículo 18.4 del texto constitucional. El tipo exige un ánimo o intención de descubrir los secretos o vulnerar la intimidad de otro. Es necesario, además, un elemento subjetivo del injusto consistente en la finalidad de perjudicar al titular de los datos o a un tercero.*
>
> *En este sentido, conforme a la jurisprudencia mayoritaria de esta Sala, es necesario hacer una interpretación sistemática del precepto entendiendo que el acceso debe realizarse en perjuicio del titular de los datos. De esta forma, en la sentencia núm. 1328/2009, de 30 de diciembre, señalábamos con relación a las conductas tipificadas en el art. 197.2 del Código Penal que "es necesario realizar una interpretación integradora en el sentido de que como en el inciso primero, se castigan idénticos comportamientos objetivos que el inciso 2º (apodere, utilice, modifique) no tendría sentido de que en el mero acceso no se exija perjuicio alguno y en conductas que precisan ese previo acceso añadiendo otros comportamientos, se exija ese perjuicio, cuando tales conductas ya serian punibles -y con la misma pena- en el inciso segundo. La solución sería -partiendo de que en el término 'tercero' debe incluirse el afectado, en su intimidad, sujeto pasivo, al que esencialmente se refiere el tipo- entender que los apoderamientos, accesos, utilizaciones o modificaciones de datos de carácter personal, realizadas en perjuicio de tercero se incluirían en el inciso inicial del art. 197.2, y en cambio, en el inciso segundo deberían ser subsumidas las conductas de acceso en perjuicio del titular de los datos".*

[70] STS 1383/2019 - ECLI:ES:TS:2019:1383, Id Cendoj: 28079120012019100277

El objeto de protección son los datos reservados de carácter personal o familiar. Conforme dispone el artículo 4.1 del 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), de aplicación directa en toda la Unión Europea a partir del 25 de mayo de 2018, ha de entenderse por "datos personales" toda información sobre una persona física identificada o identificable.

En esta misma línea, decíamos en la sentencia de este Tribunal núm. 1328/2009, de 30 de diciembre, que los datos de carácter reservado son aquellos que no son susceptibles de ser conocidos por cualquiera.

Por lo que se refiere al elemento objetivo del perjuicio ocasionado por la acción delictiva, en la sentencia núm. 1328/2009, de 30 de diciembre, distinguíamos entre datos "sensibles" y los que no lo son, precisando que los primeros son por sí mismo capaces para producir un perjuicio típico, por lo que el acceso a los mismos, apoderamiento o divulgación, poniéndolos al descubierto comporta ya ese daño a su derecho a mantener los secretos ocultos (intimidad) integrando el "perjuicio" exigido mientras que en los datos "no sensibles", no es que no tengan virtualidad lesiva suficiente para provocar para producir el perjuicio, sino que debería acreditarse su efectiva concurrencia.»

Por todo ello, sería interesante que se intentara homogeneizar el contenido de los conceptos desde el punto de vista técnico jurídico y administrativo desde el prisma de la protección de datos *(categorías especiales vs datos sensibles)* para evitar disfunciones por parte de las entidades y personas que deben moverse en este campo.

Seudonimización: Tratamiento de datos personales de forma que no se puedan atribuir la identificación a un interesado sin utilizar información adicional, siempre que la mentada información accesoria figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan directamente a una persona física identificada o identificable.

Constituye pues una medida de seguridad para evitar que ciertos datos que contribuyen a identificar a una persona se le puedan atribuir separando con barreras técnicas u organizativas los mismos para dificultar que pueda ser identificada sin contar con la información adicional que figuraría en otro registro. La implantación de dichas medidas coadyuva al responsable y al posible encargado a cumplir con sus obligaciones en materia de protección de datos.

No obstante, el uso de esta medida de seguridad no siempre garantiza la confidencialidad de los datos de carácter personal pues, en ocasiones, cabe identificar a la persona de modo indirecto, gracias a otros datos periféricos, de ahí la necesidad de seguir cumpliendo con el resto de la normativa de protección de datos respecto al tratamiento y las medidas de seguridad que deben observarse respecto a los mismos.

Unido a este concepto estaría lo que la AEPD[71] define como función resumen o función hash, que consiste en un proceso que transforma cualquier con-

[71] https://www.aepd.es/sites/default/files/2020-05/estudio-hash-anonimidad.pdf

junto arbitrario de datos en una nueva serie de caracteres con una longitud fija, independientemente del tamaño de los datos de entrada. El resultado obtenido se denomina hash, resumen, digest o imagen. Muchas veces, el término «hash» se utiliza tanto para referirse a la función hash como al valor resultado de ejecutar dicha función sobre un mensaje en particular. A los datos que van a ser procesados por la función hash se le denomina mensaje o preimagen. El conjunto de todos los posibles mensajes o preimágenes es el dominio o espacio de mensajes.

Resumiendo: es una técnica que permite tratar datos con un identificador (seudónimo-numeración) y un proceso que concluye en que si no se puede conocer otra información que sirve de nexo no se pueda identificar finalmente a la persona.

Anonimización: Forma o proceso que permite eliminar las posibilidades de identificación. De nuevo la AEPD en su Guía de *«Orientaciones y garantías en los procedimientos de anonimización de datos personales»*, de recomendada lectura, recoge que en el proceso de anonimización se deberá producir la ruptura de la cadena de identificación de las personas. Esta cadena se compone de microdatos o datos de identificación directa y de datos de identificación indirecta. Los microdatos permiten la identificación directa de las personas y los datos de identificación indirecta son datos cruzados de la misma o de diferentes fuentes que pueden permitir la reidentificación de las personas, como la información de otras bases de datos del mismo u otro responsable, de las redes sociales, buscadores, blogs, etc.

Este proceso desde un punto de vista técnico jurídico no debe confundirse con información anónima, puesto que está sería aquella que no se refiere a una persona física identificada o identificable ni a datos personales que se hayan anonimizado de forma que el interesado no sea identificable o haya dejado de serlo.

También es interesante conocer la definición de k-anonimidad, la cual, la Agencia[72] define como la propiedad de los datos anonimizados que permite cuantificar en qué medida se conserva el anonimato de los sujetos presentes en un conjunto de datos en el que se han eliminado los identificadores, es decir, es una medida del riesgo de que agentes externos puedan obtener información de carácter personal a partir de datos anonimizados (posibilidad de reidentificación)

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

Estos datos son de suma importancia para el trabajo de las autoridades competentes puesto que en muchas ocasiones son el objetivo de una inspección técnico policial y la base para poder atribuir a una persona la posible comisión de un ilícito penal. La base legal del tratamiento en el proceso penal queda fundamentalmente incluida en la LECRIM, la LOFCS, el RD 769/1987, de 19 de junio, sobre regulación de la Policía Judicial, si bien, deben cumplirse otras cuando se realicen otras funciones como la identificación de restos cadavéricos o averiguaciones en caso de desapariciones de personas.

[72] https://www.aepd.es/en/documento/nota-tecnica-kanonimidad-en.pdf

La Declaración Internacional sobre Datos Genéticos Humanos de la UNESCO 36, adoptada en el año 2003, establece una serie de normas éticas, científicas y organizativas que deben seguir la recolección, tratamiento, utilización y conservación de los datos genéticos humanos, los datos proteómicos, humanos y las muestras biológicas de las que esos datos provengan. Igualmente, la Ley 14/2007, de 3 de julio, de Investigación biomédica dispone algunas cuestiones relevantes para los interesados de forma que identifica en este campo lo que se entiende por dato genético de carácter personal: «*información sobre las características hereditarias de una persona, identificada o identificable obtenida por análisis de ácidos nucleicos u otros análisis científicos*.» Recogiendo asimismo cuestiones sobre el consentimiento informado, el derecho a la información, el derecho a no saber, la protección de datos personales, las garantías de confidencialidad, la trazabilidad y la seguridad de estos datos.

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

En el último documento del Parlamento Europeo sobre Inteligencia Artificial y Datos biométricos[73] se conceptúan las siguientes definiciones:

«Sistemas de identificación biométrica remota» que se definen como sistemas de IA utilizados con el propósito de identificar a personas físicas a distancia mediante la comparación de los datos biométricos de una persona con los datos biométricos contenidos en una base de datos de referencia, y sin conocimiento previo del usuario del sistema de IA si la persona estará presente y podrá ser identificada.

«Sistemas de reconocimiento de emociones» que se concretan como sistemas de inteligencia artificial utilizados con el fin de identificar o inferir emociones o intenciones de personas físicas sobre la base de sus datos biométricos.

«Sistemas de categorización biométrica» que podemos definir como sistemas de inteligencia artificial utilizados «con el propósito de asignar a personas físicas a categorías específicas, como sexo, edad, color de cabello, color de ojos, tatuajes, origen étnico u orientación sexual o política, sobre la base de sus datos biométricos datos»

En base a lo anterior, no se puede olvidar que las imágenes son un identificador que constituye un dato de carácter personal y los datos biométricos otro diferente que, en ciertas ocasiones, también tienen dicha consideración. De hecho, estos últimos provienen de convertir dichas imágenes o cualquier otro indicador a través de un algoritmo o plantilla que los parametriza en un número que se almacena con unas medidas de seguridad. Una vez almacenado se compara con una muestra abierta y sí el sistema detecta dicho número nos arroja una coincidencia «hit» que nos dará una probabilidad mayor o menor (score) de que la persona o parte de la persona sea la misma en ambos tratamientos.

[73] GONZALEZ FUSTER. G y Nadolna Peeters. M «Person identification, human rights and ethical principles. Rethinking biometrics in the era of artificial intelligence» PE. 697.191. ISBN: 978-92-846-8818-0

Los datos biométricos se considerarán de categoría especial únicamente cuando vayan dirigidos a identificar de manera unívoca a una persona física, ya que en caso contrario se pueden utilizar sin que concurran los presupuestos obligatorios de las categorías especiales (*Vid. dictamen 36/2020 de la AEPD y la Nota técnica de la AEPD y el EDPS, de junio de 2020, titulada «14 equívocos con relación a la identificación y autenticación biométrica»*

Resulta especialmente relevante señalar que el legislador español ha incluido una previsión específica en el artículo 13.2 de la LOPDP que otorga la justificación legal específica a que por parte de las autoridades competentes se traten datos biométricos dirigidos a identificar inequívocamente a una persona.

Datos relativos a la salud: Son aquellos datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud.

Por lo tanto, la mera asistencia a un centro hospitalario o de salud y su constatación ante terceros, mientras que no se releve información sobre la patología del interesado, no se constituiría en un dato de salud.

La Disposición adicional decimoséptima de la LOPDGDD, intitulada *«Tratamientos de datos de salud»*, recoge que los tratamientos de datos relacionados con la salud y de datos genéticos se encuentran amparados en las letras g), h), i) y j) del artículo 9.2 del RGPD, encontrándose regulados en las siguientes leyes y sus disposiciones de desarrollo:

a) La Ley 14/1986, de 25 de abril, General de Sanidad.
b) La Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales.
c) La Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.
d) La Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud.
e) La Ley 44/2003, de 21 de noviembre, de ordenación de las profesiones sanitarias.
f) La Ley 14/2007, de 3 de julio, de Investigación biomédica.
g) La Ley 33/2011, de 4 de octubre, General de Salud Pública.
h) La Ley 20/2015, de 14 de julio, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras.
i) El texto refundido de la Ley de garantías y uso racional de los 105 medicamentos y productos sanitarios, aprobado por Real Decreto Legislativo 1/2015, de 24 de julio.
j) El texto refundido de la Ley General de derechos de las personas con discapacidad y de su inclusión social, aprobado por Real Decreto Legislativo 1/2013 de 29 de noviembre.

Posteriormente dicha disposición dispone como se tratarán los datos para investigaciones en salud y enumera los criterios obligatorios a seguir.

Del mismo modo, de la lectura de la Estrategia de Salud Digital del Sistema Nacional de Salud se debe incidir en que, entre sus objetivos estratégicos, cuenta con la premisa de adoptar políticas de gestión y gobierno de los datos que permi-

tan disponer de una información interoperable y de calidad y crear un Espacio Nacional de Datos de Salud para la generación de conocimiento científico y la evaluación de los servicios.

En base a esta definición y los documentos expuestos, se puede afirmar que también se pueden y se podrán tratar datos de salud conforme a la LOPDP. A modo de ejemplo, la LECRIM recoge en sus artículos 520.2 i) y 527.3, con el fin de preservar su integridad, el derecho a la persona privada de libertad a ser reconocido por el médico forense o su sustituto legal y, en su defecto, por el de la institución en que se encuentre, o por cualquier otro dependiente del Estado o de otras Administraciones Públicas, cuyo resultado, según la Guía para la Práctica de Diligencias por la Policía Judicial aprobadas por la Comisión Nacional de Coordinación de Policía Judicial, debe incluirse en una diligencia que deberá hacer constar: la identidad del detenido para el que se requiere el reconocimiento médico, persona que lo interesa, Autoridad judicial a la que se solicita el Médico Forense, facultativo que realiza el reconocimiento, resultado del mismo y lugar de custodia del detenido. En todos los casos, se solicitará del facultativo, certificado o informe médico con el fin de adjuntarlo a las diligencias.

Del mismo modo, en su artículo 796.1ª y 7ª se prevé que la policía judicial sin perjuicio de recabar los auxilios a médicos o profesionales de la salud, solicitará del facultativo o del personal sanitario que atendiere al ofendido copia del informe relativo a la asistencia prestada (parte de lesiones o criterio médico) para su unión al atestado policial y que la práctica de las pruebas de alcoholemia se ajustará a lo establecido en la legislación de seguridad vial, si bien, las pruebas para detectar la presencia de drogas tóxicas, estupefacientes y sustancias psicotrópicas en los conductores de vehículos a motor y ciclomotores serán realizadas por agentes de la policía judicial de tráfico con formación específica y sujeción, asimismo, a lo previsto en las normas de seguridad vial. Cuando el test indiciario salival, al que obligatoriamente deberá someterse el conductor, arroje un resultado positivo o el conductor presente signos de haber consumido las sustancias referidas, estará obligado a facilitar saliva en cantidad suficiente, que será analizada en laboratorios homologados, garantizándose la cadena de custodia.

Responsable del tratamiento o responsable: La definición general se define en el RGPD y señala que será 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.[74]

En la LOPDP se refleja como responsable de tratamiento a la autoridad competente que sola o conjuntamente con otras, determine los fines y medios del tratamiento de datos personales.

Sin embargo, de hecho, en muchos casos deberá entender como la persona que se designe dentro de la estructura de las autoridades competentes para cum-

[74] Leer como cuestión de interés para completar el concepto de interesado el fallo de la Sentencia del caso Asunto C131/12 Google España S.L., Google, INC c vs Spain (AEPD), Mario Costeja González (2014)

plir con las obligaciones de dicho cargo. Siendo éstas toda autoridad pública que tenga competencias encomendadas legalmente para el tratamiento de datos personales con alguno de los fines de la LOPDP.

Como encargado de tratamiento se puede conceptualizar como la persona física o jurídica, autoridad pública, agencia u otro organismo, que trata datos personales en nombre del responsable. Existen dos condiciones básicas para calificar como encargado a una entidad: que sea un sujeto distinto y diferente en relación con el responsable y que trate los datos personales en nombre del mismo

El encargado no debe tratar los datos de otra manera que no sea de acuerdo con las instrucciones recibidas del responsable. Las instrucciones del controlador aún pueden dejar cierto grado de discreción sobre cómo servir mejor a los intereses del responsable del tratamiento, permitiendo al encargado del tratamiento elegir los medios técnicos y organizativos más adecuados. Sin embargo, éste infringiría la normativa aplicable si va más allá de las instrucciones recibidas.

En estos casos, si comienza a determinar sus propios fines y medios de procesamiento será considerado el responsable con respecto a ese tratamiento y puede estar sujeto a sanciones por dichas actuaciones.

Si una operación de tratamiento va a ser llevada a cabo por cuenta de un responsable del tratamiento, este recurrirá únicamente a encargados que ofrezcan garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento sea conforme con la legislación aplicable y garantice la protección de los derechos del interesado. El tratamiento por medio de un encargado se regirá por un contrato, convenio u otro instrumento jurídico constituido por escrito[75] que corresponda, concluidos con arreglo al Derecho de la Unión Europea o a la legislación española.

Para profundizar desde un punto de vista técnico en el alcance de estas figuras es muy recomendable acudir a las *«Guidelines 07/2020 on the concepts of controller and processor in the GDPR- Directrices sobre los conceptos de responsable y encargado de tratamiento en el RGPD»* publicadas por el CEPD el 7 de julio de 2021.

En particular, el legislador español, como se adelantó previamente, entiende como autoridad competente como toda autoridad pública con misiones o funciones directas para la prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluidas la protección y prevención frente a amenazas para la seguridad pública; o cualquier otro órgano o entidad a quien en nuestro ordenamiento jurídico haya confiado el ejercicio de la autoridad pública y las competencias públicas a efectos de prevención, investigación, detección o enjuiciamiento de infracciones penales o ejecución de sanciones penales, incluidas la protección y prevención frente a amenazas para la segu-

[75] El expediente Nº: E/12482/2021 de la AEPD, viene a determinar que: «Los acuerdos no escritos (independientemente de cuán exhaustivos o efectivos sean) no pueden considerarse suficientes para cumplir los requisitos establecidos en el artículo 28 del RGPD. No obstante, estamos ante una multinacional que implementa cláusulas y contratos estándares, por lo que se prevé que su uso efectivo iría precedido de una u otra forma de la firma y aceptación de los términos de uso de la licencia, y la información sobre el uso de los datos, incluida la necesidad de Identificación de la parte responsable del tratamiento previo al funcionamiento de las aplicaciones.»

ridad pública. Obviamente, ostentan dicha consideración las Autoridades judiciales del orden jurisdiccional penal y el Ministerio Fiscal.

Delegado de Protección de Datos (DPD): Es la nueva figura derivada del nuevo bloque de protección de datos que se conforma como piedra angular de la misma ya que el nombramiento de un DPD puede facilitar el cumplimiento y deviene en un elemento imprescindible para las organizaciones públicas y privadas[76].

Además de facilitar el cumplimiento mediante la aplicación de instrumentos de rendición de cuentas (tales como facilitar o llevar a cabo evaluaciones de impacto y auditorías de protección de datos), los DPD actúan como intermediarios entre las partes interesadas correspondientes (autoridades de control, interesados y unidades dentro de las organizaciones) de forma que se puedan llegar a soluciones que dentro de la ley puedan favorecer a todas las partes implicadas. Es figura es una herramienta más de la *autorregulación derivada de la proactividad*, generando un sistema *«win-win»* para las entidades ya se incorpore a las mismas o sea externo a la estructura de la organización.

Tanto el RGPD como la LOPDP dejan claro que es el responsable o el encargado del tratamiento quienes están obligados a garantizar y ser capaces de demostrar que el tratamiento se realiza de conformidad con la legalidad, por lo que debe quedar muy claro que los DPD no son personalmente responsables en caso de incumplimiento de la normativa o vulneración de los derechos de los interesados. Si bien, si podrían exigírseles responsabilidades por actuaciones negligentes o inobservancia de sus funciones.

Asimismo, el responsable o el encargado del tratamiento tienen un papel fundamental a la hora de posibilitar el desempeño efectivo de las tareas del DPD ya que el nombramiento o designación de un DPD es sólo un primer paso, puesto que esta figura debe disfrutar de una autonomía real y contar con los recursos suficientes para desarrollar su labor de forma efectiva.

Se reconoce al DPD como participante clave en el nuevo sistema de gestión de los datos y establece las condiciones para su nombramiento, su puesto y sus tareas.

Para conocer mejor esta figura es imprescindible acceder a la página web de la AEPD y leer el informe del WP29 243 rev.01 «*Directrices sobre los delegados de protección de datos (DPD)*»[77]o el contenido del *«Manual del DPD (Delegado de Protección de Datos) Guía para los Delegados de Protección de Datos en los sectores públicos y semi-públicos sobre cómo garantizar el cumplimiento del Reglamento General de Protección de Datos de la Unión Europea (Reglamento (UE) 2016/679)»* elaborado para el programa «T4DATA» financiado por la UE.[78]

---

[76] Esta figura, a diferencia de otros países de la Unión Europea, no era obligatoria en nuestro país. Se puede buscar un precedente en las tareas del Responsable de seguridad de los ficheros contenidas en el artículo 95 del 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.

[77] https://www.aepd.es/es/documento/wp243rev01-es.pdf

[78] Acuerdo de subvención número: 769100 – T4DATA – REC-DATA-2016/REC-DATA-2016-01

En los artículos 40 y 41 de la LOPDP esta figura queda descrita de la forma siguiente:

> *«Artículo 40. Designación del delegado de protección de datos.*
>
> *1. Los responsables del tratamiento designarán, en todo caso, un delegado de protección de datos. No estarán obligados a designarlo los órganos jurisdiccionales o el Ministerio Fiscal cuando el tratamiento de datos personales se realice en el ejercicio de sus funciones jurisdiccionales.*
>
> *2. El delegado de protección de datos será designado atendiendo a sus cualidades profesionales. En concreto, se tendrán en cuenta sus conocimientos especializados en legislación, su experiencia en materia de protección de datos y su capacidad para desempeñar las funciones a las que se refiere el artículo 42. En el caso de haber designado un delegado de protección de datos al amparo del Reglamento General de Protección de Datos, este será el que asumirá las funciones de delegado de protección de datos previstas en esta ley orgánica.*
>
> *3. Podrá designarse a un único delegado de protección de datos para varias autoridades competentes, teniendo en cuenta la estructura organizativa y el tamaño de éstas.*
>
> *4. Los responsables del tratamiento publicarán los datos de contacto del delegado de protección de datos y comunicarán a la autoridad de protección de datos competente su designación y cese, en el plazo de diez días desde que se haya producido.*
>
> *Artículo 41. Posición del delegado de protección de datos.*
>
> *1. El responsable del tratamiento velará por que el delegado de protección de datos participe adecuada y oportunamente en todas las cuestiones relativas a la protección de datos personales, al tiempo que cuidará de que mantenga sus conocimientos especializados, cuente con los recursos necesarios para el desempeño de sus funciones y acceda a los datos personales y a las operaciones de tratamiento.*
>
> *2. El delegado de protección de datos no podrá ser removido ni sancionado por el responsable o el encargado por desempeñar sus funciones, salvo que incurriera en dolo o negligencia grave en su ejercicio.*
>
> *Se garantizará la independencia del delegado de protección de datos dentro de la organización, debiendo evitar cualquier conflicto de intereses.*
>
> *3. En el ejercicio de sus funciones el delegado de protección de datos tendrá acceso a los datos personales y procesos de tratamiento. La existencia de cualquier deber de confidencialidad o secreto, no permitirá que el responsable o el encargado del tratamiento se oponga a dicho acceso.*
>
> *4. Cuando el delegado de protección de datos aprecie la existencia de una vulneración relevante en materia de protección de datos lo documentará y lo comunicará inmediatamente a los órganos de dirección del responsable o del encargado del tratamiento.*

Como cuestiones importantes a señalar en este ámbito propio serían que el DPD será único en el caso de tener que cumplir con funciones dentro del ámbito del RGPD y la LOPDP, no permitiéndose dos figuras distintas en el ámbito de las organizaciones de las autoridades competentes y que esta figura goza de una protección reforzada para el cumplimiento de sus funciones con el fin de poder cumplirlas con garantías e independencia.

Sus funciones, recogidas en el artículo 42, se detallarán junto con la Política de Seguridad de la Información y Protección de Datos Personales del Ministerio del Interior.

Para el desarrollo de las misiones de esta figura también resulta fundamental el contenido de la Instrucción 1/2021, de 2 de noviembre, de la Agencia Española de Protección de Datos, por la que se establecen directrices respecto de la función consultiva de la Agencia, de conformidad con 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 la libre circulación de esos datos, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, y el Estatuto de la Agencia Española de Protección de Datos, aprobado por el Real Decreto 389/2021, de 1 de junio, donde en su artículo cuarto establece el sistema de consultas de los DPD a la Agencia.

Este sistema podría resumirse en que la Agencia ha habilitado un canal de consulta para DPD que previamente habrán de ser notificados a la misma.

Para realizar las consultas, éstas deben ir acompañadas de un informe del DPD en cuestión, en el que se analice el tratamiento sobre el que se consulta y se examinen los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del mismo. Todo ello de conformidad con el principio de responsabilidad proactiva y del contenido de la normativa aplicable (RGPD, LOPDP o norma que corresponda). Las preguntas que no vayan acompañadas por el informe del DPD que la remite no serán atendidas, lo cual constituye un elemento de refuerzo de la figura y una criba a la hora de plantear estas cuestiones.

En estos casos, no serán objeto de respuesta las consultas:

- Que planteen tratamientos hipotéticos.
- Que estén o puedan estar relacionadas con procedimientos en tramitación en la AEPD, incluidas las relativas al estado de tramitación.
- Que pretendan la validación de actuaciones o documentos en materia de protección de datos elaborados por responsable o encargados.
- Que impliquen acceso a la información pública.
- Que se refieran a cuestiones que se encuentran ya explicadas y son accesibles en los materiales publicados en la página web de la AEPD, tales como las Guías, Preguntas Frecuentes y Herramientas elaboradas por esta entidad.

Autoridad de control: Esta se constituye en una autoridad pública independiente, como son la Agencia Española de Protección de Datos y las Agencias autonómicas.

A nivel nacional, sin perjuicio del desempeño de las funciones y potestades que le atribuyan otras leyes o normas de Derecho de la Unión Europea, corresponde a la AEPD supervisar la aplicación del RGPD, la LOPDGDD, la LOPDP, la LOPNR y la futura LOPDFIN, en particular, ejercer las funciones establecidas en el artículo 57 y las potestades previstas en el artículo 58 del antedicho reglamento, en las señaladas leyes orgánicas y en sus disposiciones de desarrollo.

El artículo 58 del RGPD atribuye a las Autoridades de control los siguientes poderes o atribuciones: Poderes de investigación, Poderes correctivos y Poderes de autorización y consultivos.

A los efectos de la LOPDP son autoridades de protección de datos independientes:

a) La Agencia Española de Protección de Datos.
b) Las autoridades autonómicas de protección de datos, exclusivamente en relación a aquellos tratamientos de los que sean responsables en su ámbito de competencia, y conforme a lo dispuesto en el artículo 57.1 de la Ley Orgánica 3/2018, de 5 de diciembre.

Estas últimas, en la actualidad, son:

- El Consejo de Transparencia y Protección de Datos como la autoridad independiente de control en materia de protección de datos y de transparencia en la Comunidad Autónoma de Andalucía.
- La Autoridad Catalana de Protección de Datos.
- La Agencia Vasca de Protección de Datos

Dichas autoridades se regirán por esta ley orgánica respecto de los tratamientos sometidos a la misma, y por lo establecido en el Título VII de la Ley Orgánica 3/2018, de 5 de diciembre, y en sus normas de creación, así como por lo que establezcan sus normas de desarrollo.

La Agencia Española de Protección de Datos actuará como representante de las autoridades de protección de datos en el Comité Europeo de Protección de Datos.

Recientemente, el Real Decreto 389/2021, de 1 de junio, por el que se aprueba el Estatuto de la Agencia Española de Protección de Datos[79] ha venido a adecuar la estructura orgánica de la Agencia a lo previsto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, en la Ley Orgánica 3/2018, de 5 de diciembre, y en la Ley Orgánica 7/2021, de 26 de mayo, resultado un instrumento eficaz y proporcionado para cumplir con este propósito, sin afectar en forma alguna a los derechos y deberes de la ciudadanía.

Si se quiere conocer cuántos países cuentan con autoridades de protección de datos se puede acudir a la relación contenida en la 41ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad[80].

Transferencia internacional: Aunque contamos con algún antevente previo[81], no existe una definición formal de transferencia internacional ni en el RGPD ni en la Directiva de datos policiales, si bien, la AEPD las define como: *«flujo de datos personales desde el territorio español a destinatarios fuera del Espacio Económico*

[79] https://www.boe.es/buscar/act.php?id=BOE-A-2021-9175

[80] https://privacyconference2019.info/about/accredited-members-and-observers/

[81] Instrucción 1/2000, de 1 de diciembre, de la Agencia de Protección de Datos, relativa a las normas por las que se rigen los movimientos internacionales de datos. Agencia de Protección de Datos «BOE» núm. 301, de 16 de diciembre de 2000. Referencia: BOE-A-2000-22726

Europea (los países de la Unión Europea más Liechtenstein, Islandia y Noruega)». Nosotros podremos definirlas a nivel general como la remisión, a través de cualquier medio, de datos personales desde un Estado miembro de la Unión Europea hacía un tercer estado o una organización internacional.

Sin embargo, el Convenio 108 + ha establecido en su artículo 14 que serían transferencias de datos personales aquellas que sean objeto de tratamiento o vayan a serlo tras su transmisión a un tercer país u organización internacional. En este caso, la transferencia: *«...(...)...solo puede tener lugar cuando se asegure un nivel apropiado de protección basado en las disposiciones del presente Convenio.»*

El Derecho de la Unión, contiene disposiciones que establecen la libre circulación de los datos dentro de su territorio y del Espacio Económico Europeo (EEE), la posibilidad de transferencias a terceros estados u organizaciones internacionales que garanticen un nivel adecuado de protección y los requisitos para éstas cuando se considera que los estados no ofrecen un nivel adecuado de protección si el responsable o encargado adopta las medidas oportunas o cuando concurren una serie de excepciones para situaciones específicas.

Estas cuestiones se pueden analizar pormenorizadamente en la información que facilita la AEPD, si bien, ya sea mediante el sistema de decisiones de adecuación, garantías adecuadas, excepciones o autorización expresa de la Agencia, las referencias incorporadas en dicha documentación están referidas al RGPD prácticamente en su totalidad.

¿Cuál sería el resumen del contenido de la normativa? Pues que los responsables del tratamiento podrán realizar transferencias internacionales de datos sin autorización de la AEPD siempre que el tratamiento de datos observe lo siguiente:

- Transferencias basadas en una decisión de adecuación: Cuando las entidades receptoras de los datos se encuentren en un país, un territorio o uno o varios sectores específicos de ese país u organización internacional que hayan sido declarados de nivel de protección adecuado por la Comisión Europea. En ese caso resulta un instrumento significativo las *«Recomendaciones 01/2021 relativas a las referencias sobre adecuación en el marco de la Directiva sobre protección de datos en el ámbito penal»*[82].
- Mediante la aportación de garantías adecuadas: A falta de decisión de adecuación si se ofrecen garantías adecuadas contenidas en la normativa.
- Excepciones para situaciones específicas: Si no existe una decisión de adecuación o no se pueden aportar las garantías adecuadas, sólo se podrán realizar si se cumplen una serie de condiciones que se encuentran contenidas en el artículo 49 del RGPD y 46 y 47 de 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.
- Con autorización de la AEPD: cuando el ofrecimiento de garantías adecuadas se realice mediante cláusulas contractuales entre el responsable o el

[82] https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012021-adequacy-referential-under-law_es

encargado y el responsable, encargado o subencargado, que no hayan sido adoptadas por la Comisión Europea o por la Agencia Española de Protección de Datos y aprobadas por la Comisión Europea o en Disposiciones que se incorporen en acuerdos administrativos entre las autoridades u organismos públicos que incluyan derechos efectivos y exigibles para las personas interesadas.

- Normas Corporativas Vinculantes (BCR): Las normas corporativas vinculantes serían *«las políticas de protección de datos personales asumidas por un responsable o encargado del tratamiento establecido en el territorio de un Estado miembro para transferencias o un conjunto de transferencias de datos personales a un responsable o encargado en uno o más países terceros, dentro de un grupo empresarial o una unión de empresas dedicadas a una actividad económica conjunta».*

La única decisión de adecuación en el ámbito de la DDP y por lo tanto la que se puede aplicar actualmente en el ámbito de la LOPDP es la siguiente: *Commission Implementing Decision, of 28.6.2021, pursuant to Directive (EU) 2016/680 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom."*

Como cuestión relevante, cabe apuntar que el TJUE (*Asunto Lindquist, C-101/01)* determinó que no existe transferencia a tercer país cuando una persona de un Estado miembro cargue los datos personales en una página de Internet que se almacenan en un dominio de Internet en el que la página puede ser consultada y que se alojada por una persona física o jurídica establecida en dicho Estado o en otro Estado miembro, con lo que los datos quedan accesibles a toda persona que se conecte a la red, incluidas la personas de un tercer país. O lo que es lo mismo, subir datos personales a una web no es una transferencia internacional.

Un concepto interesante a desarrollar en relación con estas actuaciones sería el de *«Transfer Impact Assessment (TIA)»* o Evaluación de Impacto de transferencias internacionales. Tras la Sentencia del Asunto «Schrems» (C-362/14) del TJUE que derivo en la inaplicación del Escudo de Privacidad con los Estados Unidos de América derivó en una figura importante, la TIA, de manera que se evaluase caso por caso y de manera global si la protección de datos de un tercer estado garantiza dicha seguridad para los interesados. Es decir, se debe ir más allá de valorar si el Estado posee normativa sobre esta materia abordando la información sobre si dicha normativa está implantada y aplicada y, sobre todo, que garantías se establecen en los supuestos de remisión a terceros Estado de los datos transferidos.

Tratamiento transfronterizo: El RGPD los define como: *«el tratamiento de datos personales realizado en el contexto de las actividades de establecimientos en más de un Estado miembro de un responsable o un encargado del tratamiento en la Unión, si el responsable o el encargado está establecido en más de un Estado miembro, o b) el tratamiento de datos personales realizado en el contexto de las actividades de un único establecimiento de un responsable o un encargado del tratamiento en la Unión, pero que afecta sustancialmente o es probable que afecte sustancialmente a interesados en más de un Estado miembro.»* En el marco de la Directiva

será pues el tratamiento realizado por autoridades competentes en base a los fines de la misma dentro del territorio de la Unión.[83]

Elaboración de perfiles: toda forma de tratamiento automatizado (por tanto no cabe en esta definición el llevado a cabo en otros supuestos) de datos personales consistente en utilizar datos personales con el objetivo de evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física. En este aspecto se debe analizar el contenido del artículo 14 de la LOPDP y la evolución que tendrá junto con el futuro reglamento UE que regule el uso de la inteligencia artificial.

Como resumen simplificado se puede señalar que existirían tres formas principales de elaboración de perfiles:

- Con carácter general
- Decisiones basadas en la elaboración de perfiles
- Decisiones basadas únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que producen efectos jurídicos en el interesado o que le afecten significativamente.

Los responsables pueden llevar a cabo esta actuación y adoptar decisiones automatizadas siempre que cumplan todos los principios y requisitos legales pertinentes (base legitimadora, etc.). En los supuestos de decisiones basadas únicamente en los tratamientos automatizados, que incluyan la elaboración de perfiles, se aplicaran las garantías y restricciones adicionales que eleven las garantidas de los interesados.

Violación de la seguridad de los datos personales: la LOPDP la define como toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita, o la comunicación o acceso no autorizados a datos personales transmitidos, conservados o tratados de otra forma. Estas violaciones de seguridad, en algunos supuestos, venimos a denominarlas *«Brechas de Seguridad»*. Estas brechas, desde un punto de vista técnico jurídico serían aquellos incidentes de seguridad que ocasionan la destrucción, pérdida o alteración accidental o ilícita de los datos personales tratados por un responsable, o bien la comunicación o acceso no autorizados a los mismos.

Una brecha de datos personales puede tener una serie de efectos adversos considerables en las personas, susceptibles de ocasionar daños y perjuicios físicos, materiales o inmateriales; por lo que hay que intentar evitarlas y en caso de que sucedan gestionarlas adecuadamente, especialmente cuando puedan poner en riesgo los derechos y libertades de las personas físicas.

[83] COM (2021) 206 final de 21 de abril de 2021. Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (ley de inteligencia artificial) y se modifican determinados actos legislativos de la Unión.

La normativa aplicable atribuye a los responsables de un tratamiento de datos personales la obligación de notificar a la autoridad de control competente las brechas de datos personales cuando sea probable que constituyan un riesgo para los derechos y libertades de las personas. Si éste entiende que no se generan riesgos para los derechos y libertades de los interesados, aunque no se comuniquen a las autoridades de control, tiene la obligación de documentar cualquier violación de la seguridad, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas de manera que quede el suceso a disposición de estas autoridades.

Es interesante para estos supuestos la consulta de las Directrices 01/2021 del CEPD sobre ejemplos relacionados con la notificación de violación de datos personales (Versión 14 diciembre 2021), la última versión de la *«Guía para la notificación de brechas de datos personales»* de la AEPD, ya que es un documento que tiene como objetivo guiar a las personas responsables de los tratamientos de datos personales en su obligación de notificar éstas a las autoridades de protección de datos y comunicárselo a las personas cuyos datos se hayan visto afectados (supuesto que analizaremos en el apartado relativo a los derechos de los ciudadanos) y el Sistema electrónico de notificación de brechas de seguridad de la sede virtual de la propia Agencia.

IV. PRINCIPIOS DE TRATAMIENTO Y BASES DE LEGITIMACIÓN

1. Principios de tratamiento

Como hemos mencionado previamente, la evolución de la normativa en esta materia durante los últimos decenios ha sido vertiginosa, si bien, es importante señalar que la misma se ha ido basando en unos u otros principios en función de las realidades sociales que se han ido produciendo a cada paso.

Al igual que ocurre en otras ramas del Derecho en nuestro ordenamiento, donde la ley, la costumbre y los principios generales constituyen sus fuentes, una de las bases que siempre se mencionan a la hora de interpretar las normas es entender cuáles son los orígenes o los principios superiores que inspiran las disposiciones normativas.

En este caso, los principios serían el horizonte o el soporte teleológico básico o fundamental donde se puedan apoyar los que desarrollan, aplican e interpretan las normas, constituyéndose en una parte esencial y relevante del derecho a la protección de datos y resultando que, a través de los mismos, se configura un sistema de tutela que da garantías a la utilización más legítima y razonable de los datos personales[84].

Es importante que las autoridades competentes y responsables de tratamiento se centren en conocer y dominar estos principios. Las leyes cambian, pero los principios, debidamente actualizados, transcienden a aquellas y continúan siendo clave para lograr un tratamiento lícito, leal y transparente de los datos personales[85].

Durante la 31 Conferencia Internacional de Autoridades de Protección de Datos y Privacidad celebrada el 5 de noviembre de 2009 en Madrid, se presentó la Propuesta Conjunta para la Redacción de Estándares Internacionales para la protección de la Privacidad, en relación con el Tratamiento de Datos de carácter personal.

La labor conjunta de los garantes de la privacidad de casi cincuenta países, bajo coordinación de la Agencia Española de Protección de Datos, desembocó en un texto que trató de plasmar los múltiples enfoques que admitía la protección de este derecho, integrando legislaciones de los cinco continentes. El carácter consensuado aportaba dos valores añadidos esencialmente novedosos: de un lado, enfatizaba la vocación universal de los principios y garantías que configuran este derecho; del otro, reafirmaba la factibilidad de avanzar hacia un documento internacionalmente vinculante, que contribuyese a una mayor protección de los derechos y libertades individuales en un mundo globalizado, y por ello, caracterizado por las transferencias internacionales de información.

---

[84] PUYOL MONTERO. J, Los principios del derecho a la protección de datos, Capítulo IX. «Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad» Editorial Reus, 2016. 1ª Edición.

[85] https://diariolaley.laleynext.es/Content/Documento.aspx?params=H4sIAAAAAAAE-AMtMSbH1czUwMDAyNLc0MLNUK0stKs7Mz7M1AooYmBoYq-Xlp6SGuDjblualpKZl-5qWmgJRkplW65CeHVBak2qYl5hSnqqUm5edno5gUDzMBACFtAZhjAAAAWKE

En ese documento se recogían los siguientes principios básicos:

- El principio de lealtad y legalidad.
- El principio de finalidad.
- Principio de proporcionalidad.
- Principio de calidad
- Principio de transparencia
- Principio de responsabilidad
- Principio general de legitimación.

Posteriormente, derivado del RGPD, la LOPDGDD y la LOPDP, los principios actuales que rezan en ese campo serían:

- Principio de lealtad
- Principio de transparencia
- Principio de licitud del tratamiento
- Principio de limitación de la finalidad
- Principio de Minimización
- Principio de exactitud
- Principio de limitación del plazo de conservación
- Principio de seguridad de la información o confidencialidad.
- Principio de proactividad por parte del responsable (Accountability)
- Principio de privacidad por diseño y por defecto.

Como puede observarse la mayoría derivan de aquellos acordados en la Conferencia de Madrid con las adaptaciones necesarias tras más de un lustro de evolución.

Más recientemente se puede analizar el contenido del informe del Comité Jurídico Interamericano (cji): *«Principios actualizados del Comité Jurídico Interamericano sobre la privacidad y la protección de datos personales, con anotaciones.»,* de 8 de abril de 2021, que tuvo por finalidad el actualizar los *«Principios sobre la Privacidad y la Protección de Datos Personales (con anotaciones)»* adoptados por este Comité en 2015, con el objetivo de basarlos en normas y estándares reconocidos a nivel internacional, según han evolucionado hasta el año 2020. Con esta actuación se pretendía que los aprobase la Organización de Estados Americanos (OEA) y los incorporasen al acervo de esta entidad y, por lo tanto, posteriormente a los ordenamientos internos de los Estados que la conforman. Hay que tener en cuenta que, en la actualidad, casi todos los Estados Miembros de la OEA han adoptado algún tipo de legislación con respecto a la protección de la privacidad y los Datos Personales, aunque sus disposiciones varían en lo que se refiere a su enfoque, ámbito de aplicación y contenido.

Los principios específicos del tratamiento en el ámbito de los datos policiales vienen explicados en el considerando 26 e incluidos en su mayor parte en la par-

te dispositiva y en el artículo 4[86] de la DDP y el artículo 6 de la LOPDP, donde en sus apartados 1 y 5 taxativamente se viene disponer que[87]:

> *«1. Los datos personales serán:*
> *a) Tratados de manera lícita y leal.*
> *b) Recogidos con fines determinados, explícitos y legítimos, y no serán tratados de forma incompatible con esos fines.*

---

[86] Considerando 26: *«Todo tratamiento de datos personales debe ser lícito, leal y transparente en relación con las personas físicas afectadas, y únicamente podrá llevarse a cabo con los fines específicos previstos en la ley. Ello no impide, per se, que las autoridades policiales puedan llevar a cabo actividades tales como las investigaciones encubiertas o la videovigilancia. Tales actividades pueden realizarse con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y prevención frente a las amenazas para la seguridad pública, siempre y cuando estén previstas en la legislación y constituyan una medida necesaria y proporcionada en una sociedad democrática, con el debido respeto a los intereses legítimos de la persona física afectada. El principio de tratamiento leal en materia de protección de datos es un concepto distinto del derecho a un "juicio imparcial", según se define en el artículo 47 de la Carta y en el artículo 6 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales (en lo sucesivo, «CEDH»). Debe informarse a las personas físicas de los riesgos, reglas, salvaguardias y derechos aplicables en relación con el tratamiento de sus datos personales, así como del modo de hacer valer sus derechos en relación con dicho tratamiento. En particular, los fines específicos a los que obedezca el tratamiento de los datos personales deben ser explícitos y legítimos, y deben determinarse en el momento de la recopilación de los datos personales. Los datos personales deben ser adecuados y pertinentes en relación con los fines para los que se tratan, lo cual requiere, en particular, que se garantice que los datos personales recogidos no son excesivos ni se conservan más tiempo del que sea necesario para los fines con los que se tratan. Los datos personales solo deberían ser objeto de tratamiento si la finalidad del tratamiento no puede lograrse razonablemente por otros medios. Para garantizar que los datos no se conservan más tiempo del necesario, el responsable del tratamiento ha de establecer plazos para su eliminación o revisión periódica. Los Estados miembros deben establecer las salvaguardias adecuadas en relación con los datos personales almacenados por períodos más largos para su archivo por cuestiones de interés público o para su uso científico, estadístico o histórico.»* y *«Artículo 4. Principios relativos al tratamiento de datos personales. 1. Los Estados miembros dispondrán que los datos personales sean: a) tratados de manera lícita y leal; b) recogidos con fines determinados, explícitos y legítimos, y no ser tratados de forma incompatible con esos fines; c) adecuados, pertinentes y no excesivos en relación con los fines para los que son tratados; d) exactos y, si fuera necesario, actualizados; se habrán de adoptar todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que son tratados; e) conservados de forma que permita identificar al interesado durante un período no superior al necesario para los fines para los que son tratados; f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidentales, mediante la aplicación de medidas técnicas u organizativas adecuadas. 2. Se permitirá el tratamiento de los datos personales, por el mismo responsable o por otro, para fines establecidos en el artículo 1, apartado 1, distintos de aquel para el que se recojan en la medida en que: a) el responsable del tratamiento esté autorizado a tratar dichos datos personales para dicho fin de conformidad con el Derecho de la Unión o del Estado miembro, y b) el tratamiento sea necesario y proporcionado para ese otro fin de conformidad con el Derecho de la Unión o del Estado miembro. 3. El tratamiento por el mismo responsable o por otro podrá incluir el archivo en el interés público, el uso científico, estadístico o histórico para los fines establecidos en el artículo 1, apartado 1, con sujeción a las salvaguardias adecuadas para los derechos y libertades de los interesados. 4. El responsable del tratamiento será responsable y capaz de demostrar el cumplimiento de lo dispuesto en los apartados 1, 2 y 3.»*

[87] FERNÁNDEZ GONZÁLEZ. C, AYLLÓN SANTIAGO, H. Prólogo: Jorge Álvaro Navas Elorza *«Tratamiento de datos de carácter personal en el ámbito policial» ISBN:978-84-290-2433-3 Editorial Reus. 1ª Edición.*

c) Adecuados, pertinentes y no excesivos en relación con los fines para los que son tratados.

d) Exactos y, si fuera necesario, actualizados. Se adoptarán todas las medidas razonables para que se supriman o rectifiquen, sin dilación indebida, los datos personales que sean inexactos con respecto a los fines para los que son tratados.

e) Conservados de forma que permitan identificar al interesado durante un período no superior al necesario para los fines para los que son tratados.

f) Tratados de manera que se garantice una seguridad adecuada, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental. Para ello, se utilizarán las medidas técnicas u organizativas adecuadas....(...)

...(...)....5. El responsable del tratamiento deberá garantizar y estar en condiciones de demostrar el cumplimiento de lo establecido en este artículo.»

Dado el contenido de este artículo se puede afirmar con un poco más de detalle que estos datos deben ser tratados de forma que el responsable del tratamiento aplique medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con la normativa aplicable lo que constituye el principio de responsabilidad proactiva (diligencia debida).

En términos prácticos, este principio requiere que las organizaciones analicen qué datos tratan, con qué finalidades lo hacen y qué tipo de operaciones de tratamiento llevan a cabo. A partir de este conocimiento deben determinar de forma explícita la forma en que aplicarán las medidas previstas, asegurándose de que esas medidas son las adecuadas para cumplir con la legalidad y de que pueden demostrarlo ante los interesados y ante las autoridades de supervisión.[88]

Esta «*diligencia debida*» según la AEPD[89], puede definirse como *«la medida de prudencia, actividad o asiduidad que cabe razonablemente esperar, y con la que normalmente actúa, una organización prudente y razonablemente en unas circunstancias determinadas; no se mide por una norma absoluta, sino dependiendo de los hechos relativos del caso en cuestión»*; resulta pues un proceso en continua observación y prevención de los efectos negativos de las actividades de las entidades sobre la protección de datos y se compone de cuatro elementos: identificar, prevenir, mitigar y la rendición de cuentas, es decir:

1. Una evaluación del impacto real y potencial de las actividades sobre los datos (evaluación de riesgos).
2. La integración de las conclusiones, y la actuación al respecto (los controles).
3. El seguimiento y monitoreo (evaluación del desempeño).
4. La comunicación de la forma en que se hace frente a las consecuencias negativas (rendición de cuentas).

[88] «Guía del Reglamento General de Protección de Datos para responsables de tratamiento». AEPD, Autoridad Catalana de Protección de Datos y Agencia Vasca de Protección de datos. https://www.aepd.es/sites/default/files/2019-09/guia-rgpd-para-responsables-de-tratamiento.pdf

[89] Expediente Nº: PS/00392/2020

En síntesis, este principio exige una actitud consciente, diligente y proactiva por parte de las entidades frente a todos los tratamientos de datos personales que lleven a cabo y ostentar la capacidad de acreditar tales actuaciones de manera que se proporcionará una defensa contra la responsabilidad, permitirá una reducción de las sanciones o brindará un recurso de defensa cuando la entidad pueda probar que había implementado los procedimientos adecuados para prevenir un impacto negativo[90].

La AEPD[91] entiende que para poder acreditar diligencia debida, la entidad debe demostrar que ha dado todos los pasos razonables y llevado a cabo las acciones necesarias para evitar que se genere un impacto negativo. Ello se interpretará dependiendo de las circunstancias concretas de cada caso.

La normativa aplicable pretende que se anticipe el momento en que el responsable o encargado del tratamiento actúe con diligencia debida, mediante este principio de responsabilidad proactiva, gestionando los riesgos mediante un sistema de control interno sólido, que permita acreditar esta actuación diligente con carácter previo, lo cual inicialmente, pueda presentar cierta incertidumbre en su aplicación, debido al paso de un sistema cerrado, basado en una enumeración específica de las medidas de seguridad a implantar en función de la tipología de datos tratados, a un sistema abierto, cuyo objetivo es la aplicación de las medidas técnicas y organizativas *«apropiadas»* para garantizar y poder demostrar que el tratamiento es adecuado conforme al ámbito, el contexto y los fines del tratamiento.

Para el cumplimiento del principio de *«Responsabilidad Proactiva»* el responsable y encargado de tratamiento deberán previamente realizar un análisis y estudio del cumplimiento en materia de protección de datos basado en el riesgo. Es decir, deberán analizar qué medidas de protección de datos son necesarias implantar para garantizar el cumplimiento, en función de naturaleza, alcance, contexto y finalidades del tratamiento de datos que realicen, así como de los riesgos (probabilidad y consecuencia) de intromisión en los derechos y libertades de los interesados.

De esta manera cuanto más probable y mayores sean las consecuencias del riesgo del tratamiento, más medidas u de mayor calado deberán ser las necesarias a implantar un sistema para contrarrestarlas (recordando que no se trata únicamente de medidas de seguridad técnica, sino que deben venir acompañadas de las medias organizativas oportunas). Sistema que estará integrado por distintas políticas o procesos internos de privacidad que deberán ser actualizados y auditados periódicamente de manera que permitan demostrar la observancia de la normativa.

Es notable la valoración que ha hecho el TS[92] de este concepto puesto que entiende que la obligación de los responsables de adoptar las medidas de seguridad oportunas no puede ser considerada una obligación de resultado. El Alto Tribunal entiende que lo que resulta exigible es la adopción de las medidas técnicas y organizativas que, de acuerdo con el estado de la tecnología y en base a la finalidad del tratamiento y de los datos en cuestión, cumplan razonablemente con la obligación de evitar que se afecte al principio de confidencialidad (integridad,

[90] Expediente Nº: PS/00392/2020
[91] Expediente Nº: PS/00392/2020
[92] STS. 543/2022. ECLI:ES:TS.2022: 543. Cendoj:28079130032022100030.

disponibilidad y confidencialidad de los datos). Lo realmente relevante es que se asienta que no es suficiente con el diseño de las medidas, sino que es ineludible su correcta implantación y utilización de forma apropiada, de modo que, la entidad responderá por la falta de diligencia en el uso de los sistemas o programas de seguridad, entendiendo esa diligencia como aquella que sea razonable atendiendo al caso concreto.

Igualmente se exige que los datos sean tratados de manera lícita y leal (principios de licitud y lealtad): En estos supuestos no se debe confundir legalidad con lealtad puesto que esta última tiene que interpretarse como la actuación que garantiza la información oportuna al interesado, de forma que éste entienda, sin lugar a dudas, cuál va a ser el tratamiento y su extensión (y no otro u otros)

Es necesario que le quede claro que no estamos recogiendo, utilizando o tratando de cualquier otra forma los datos. Aunque no figura específicamente en este artículo 6, también debe actuarse conforme al principio de transparencia, ya que quedaría incardinado igualmente en las obligaciones del responsable a través del principio y derecho a la información. Por todo ello, se debe actuar de modo que toda información y comunicación relativa al tratamiento de datos sea fácilmente accesible, fácil de entender y que se utilice un lenguaje sencillo y claro (no técnico) adaptado, si es posible, a los destinatarios. Esta trasparencia se refiere en particular a la información de los interesados sobre la identidad del responsable del tratamiento, los fines del mismo y a la información añadida para garantizar un tratamiento honesto y diáfano con respecto a las personas físicas afectadas y a su derecho a obtener confirmación y comunicación de los datos personales que les conciernan y que son objeto de tratamiento, si bien, en este caso quedaría modulado por la excepciones legales oportunas para garantizar los fines específicos de los responsables (prevenir, investigar o detectar ilícitos penales o proteger y prevenir a la sociedad contra amenazas a la seguridad pública).

En cuanto al principio de licitud se debe entender como aquel que obliga a tratar los datos con arreglo o conforme a las leyes vigentes, lo cual, sólo se producirá en la medida en que sea necesario para la ejecución de una tarea realizada por una autoridad competente, para los fines policiales y esté basado en el Derecho de la Unión o el de los Estados miembros. Como se explica a continuación, las bases de legitimación del RGPD no coinciden con esta base única, por lo que se debe hacer un ejercicio de interpretación y aplicación más concreto, es decir, existe una gran variedad de normas legales que recogen obligaciones necesarias para cumplir con las misiones que tienen las autoridades competentes con fines policiales por lo que es importante tener claro en cada actuación cuál es el precepto legal que la ampara. No será igual fundamentar la legitimación para tratar datos personales para el acceso a una instalación bajo protección de las FCS que hacerlo para remitir tales datos a una autoridad por la comisión de una infracción administrativa o penal, siendo el tratamiento el mismo: *obtener los datos de identificación de los interesados*.

Es muy relevante señalar que la Directiva puntualiza en sus considerandos 35 y 37, que el consentimiento no constituye un fundamento jurídico para el tratamiento de los datos personales por las autoridades competentes y que tal requisito no puede legitimar por si solo el tratamiento de categorías especiales de datos. Sin embargo, en muchas ocasiones, este requerimiento puede confundirse con

algunas situaciones procesales o policiales que exigen tal condición, si bien, una vez se otorga ese formalismo (consiente la diligencia), los datos personales se tratan por imperio de la ley y no por que el interesado consienta el acto a actuación a llevar a cabo (ej.: toma de ADN o entrada y registro en un domicilio)

El artículo 11 de la LOPDP dispone:

> *«Artículo 11. Licitud del tratamiento.*
>
> *1. El tratamiento sólo será lícito en la medida en que sea necesario para los fines señalados en el artículo 1 y se realice por una autoridad competente en ejercicio de sus funciones.*
>
> *2. Cualquier ley que regule tratamientos de datos personales para los fines incluidos dentro del ámbito de aplicación de esta ley orgánica deberá indicar, al menos, los objetivos del tratamiento, los datos personales que vayan a ser objeto del mismo y las finalidades del tratamiento.»*

Los datos serán recogidos con fines determinados, explícitos y legítimos, y no serán tratados de forma incompatible con esos fines, lo que viene a ser el principio de finalidad, que consiste en que podrán recogerse datos con las finalidades apuntadas, siempre que dicha actuación sea determinada (no genérica), explicita (no pueden generar dudas o confusión al interesado) y legítima (conforme a derecho como se apuntaba) e igualmente podrán tratarse posteriormente si se hace de forma compatible con dichas premisas.

Para el caso concreto de este principio, los apartados 2, 3 y 4 del aludido artículo 6 disponen:

> *«2. Los datos personales recogidos por las autoridades competentes no serán tratados para otros fines distintos de los establecidos en el artículo 1, salvo que dicho tratamiento esté autorizado por el Derecho de la Unión Europea o por la legislación española. Cuando los datos personales sean tratados para otros fines, se aplicará el Reglamento General de Protección de Datos y la Ley Orgánica 3/2018, de 5 de diciembre, a menos que el tratamiento se efectúe como parte de una actividad que quede fuera del ámbito de aplicación del Derecho de la Unión Europea.*
>
> *3. Los datos personales podrán ser tratados por el mismo responsable o por otro, para fines establecidos en el artículo 1 distintos de aquel para el que hayan sido recogidos, en la medida en que concurran cumulativamente las dos circunstancias siguientes:*
>
> *a) Que el responsable del tratamiento sea competente para tratar los datos para ese otro fin, de acuerdo con el Derecho de la Unión Europea o la legislación española.*
>
> *b) Que el tratamiento sea necesario y proporcionado para la consecución de ese otro fin, de acuerdo con el Derecho de la Unión Europea o la legislación española.*
>
> *4. El tratamiento por el mismo responsable o por otro podrá incluir el archivo por razones de interés público, y el uso científico, estadístico o histórico para los fines establecidos en el artículo 1, con sujeción a las garantías adecuadas para los derechos y libertades de los interesados.»*

Los datos serán adecuados, pertinentes y no excesivos en relación con los fines para los que son tratados; esto constituye el principio de minimización

que podemos describir como aquel por el que que los datos tratados son los imprescindibles para poder realizar el tratamiento, además de esto, garantiza que los fines no puedan lograrse de otra forma y que únicamente deben ser los que conduzcan a la consecución de la finalidad y ni un solo datos más. No pueden almacenarse datos con la finalidad de acumular información o *«por si acaso»*. De igual modo, junto con el principio de limitación del plazo de conservación, este principio garantiza que se limite a un mínimo estricto su plazo de conservación (Vid. art.8 de la LOPDP)

Los datos serán exactos y, si fuera necesario, actualizados, que deriva en el principio de exactitud, el cual impone la obligatoriedad de adoptar todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos o incompletos con respecto a los fines para los que son tratados. Esto conlleva la obligación de los responsables de mantener los datos exactos, completos y de acomodarlos en todo supuesto que lo haga necesario.

Dentro de este principio también nos encontramos con la obligación de verificación de la calidad de los datos que se pueden comunicar a terceros. Así, el legislador dispone que las autoridades competentes adopten todas las medidas razonables para garantizar que los datos personales que sean inexactos, incompletos o que no estén actualizados no se transmitan ni se pongan a disposición de terceros. Para ello, dentro de lo que sea practicable, se controlará la calidad de los datos personales antes de transmitirlos o ponerlos a disposición de éstos y, en la medida de lo posible, en todas las transmisiones de datos personales se añadirá la información necesaria a modo de reparo o advertencia para que la autoridad competente receptora pueda valorar en qué medida los datos personales son exactos, completos y fiables y en qué medida están actualizados.

En el supuesto de que se hubieran transmitido datos personales incorrectos o se hubieran transmitido ilegalmente, el hecho deberá ponerse en conocimiento del destinatario sin dilación indebida y éste procederá a rectificar, suprimir o, en su caso, limitar el tratamiento hasta que se constate o se salve la situación.

En la LOPDP se intenta clarificar esta cuestión en su artículo 10 incidiendo en la diferencia entre datos basados en hechos o en apreciaciones subjetivas (indicios):

> *«Artículo 10. Verificación de la calidad de los datos personales.*
>
> *1. El responsable del tratamiento, en la medida de lo posible, establecerá una distinción entre los datos personales basados en hechos y los basados en apreciaciones personales.*
>
> *2. Las autoridades competentes adoptarán todas las medidas razonables para garantizar que los datos personales que sean inexactos, incompletos o no estén actualizados, no se transmitan ni se pongan a disposición de terceros. En toda transmisión de datos se trasladará al mismo tiempo la valoración de su calidad, exactitud y actualización.*
>
> *En la medida de lo posible, en todas las transmisiones de datos personales se añadirá la información necesaria para que la autoridad competente receptora pueda valorar hasta qué punto son exactos, completos y fiables, y en qué medida están actualizados. Igualmente, la autoridad competente transmisora controlará la calidad de los datos personales antes de transmitirlos o ponerlos a disposición de terceros.*

3. Si se observara que los datos personales transmitidos son incorrectos o que se han transmitido ilegalmente, estas circunstancias se pondrán en conocimiento del destinatario sin dilación indebida. En tal caso, los datos deberán rectificarse o suprimirse, o el tratamiento deberá limitarse de conformidad con lo previsto en el artículo 23.»

Los datos serán conservados de forma que permita identificar al interesado durante un período no superior al necesario para los fines para los que son tratados. Este principio lo denominamos principio de limitación de plazo de conservación y exige que no puedan conservarse o mantenerse datos durante más tiempo del necesario para los fines del tratamiento, que estos plazos deben fijarse por el responsable del tratamiento, que estos plazos podrán ampliarse en varios supuestos (investigaciones, conservación para depurar responsabilidades, etc.), que dichos plazos deben conocerse por los interesados, que las normas de los procedimientos internos garantizarán el cumplimiento de dichos plazos y que tras superarse éstos solo podrán conservarse los datos de manera disociada y estarán bloqueados.

Hay que tener en cuenta que no es lo mismo la supresión de los datos de un sistema o de su enlace (derecho al olvido) que su destrucción, ya que son dos actuaciones y fases completamente diferentes. Los datos pueden suprimirse de un sistema de modo que ningún operador sin privilegios especiales pueda acceder a los mismos y quedar bloqueado otro cierto tiempo hasta su destrucción con las medidas adecuadas de seguridad.

Esto es así porque las responsabilidades derivadas del tratamiento de los datos normalmente tienen periodos de prescripción mayores que los plazos de conservación en los sistemas.

Si se destruyeran, en muchas ocasiones, la investigación de un posible mal uso podría perjudicar a la víctima o interesado y beneficiar al infractor, cuestión esta que debe tenerse en consideración ya que el paradigma actual nos obliga a valorar el riesgo en base a los distintos perjuicios o daños que se le puedan causar al interesado en las operaciones de tratamiento de sus datos (Vid. ídem. Art. 8 LOPDP[93])

Tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidentales, mediante la aplicación de medidas técnicas u organizativas adecuadas, es lo que comprende el principio de

[93] Artículo 8. *«Plazos de conservación y revisión. 1. El responsable del tratamiento determinará que la conservación de los datos personales tenga lugar sólo durante el tiempo necesario para cumplir con los fines previstos en el artículo 1. 2. El responsable del tratamiento deberá revisar la necesidad de conservar, limitar o suprimir el conjunto de los datos personales contenidos en cada una de las actividades de tratamiento bajo su responsabilidad, como máximo cada tres años, atendiendo especialmente en cada revisión a la edad del afectado, el carácter de los datos y a la conclusión de una investigación o procedimiento penal. Si es posible, se hará mediante el tratamiento automatizado apropiado. 3. Con carácter general, el plazo máximo para la supresión de los datos será de veinte años, salvo que concurran factores como la existencia de investigaciones abiertas o delitos que no hayan prescrito, la no conclusión de la ejecución de la pena, reincidencia, necesidad de protección de las víctimas u otras circunstancias motivadas que hagan necesario el tratamiento de los datos para el cumplimiento de los fines del artículo 1.»*

seguridad de los datos. La finalidad de este principio es que los datos objeto de tratamiento no sean revelados, divulgados, difundidos o conocidos por ninguna persona o entidad ajena, fuera de los casos autorizados por la Ley, que permanezcan completos, sin que puedan perderse, destruirse o dañarse y que estén disponibles cuando se requiera.

Las obligaciones en materia de seguridad del responsable de tratamiento en base a tratamientos del RGPD vienen recogidas en sus artículos 25, 32 y 35 principalmente e igualmente dichas previsiones se han recogido en la DDP y plasmado en la LOPDP directamente en sus artículos 27, 28, 33, 35 y 37.

Las dimensiones específicas de seguridad en este campo serían la confidencialidad, la disponibilidad y la integridad; no obstante, se deben completar en el caso de tratamientos por medios electrónicos con la autenticación y la trazabilidad. Sin obviar, en ningún caso, el requisito específico de desarrollar el resto las medidas técnicas y organizativas que permitan acreditar la protección de los bienes jurídicos protegidos en juego.

El artículo 37 enumera las siguientes:

> *«1. El responsable y el encargado del tratamiento, teniendo en cuenta el estado de la técnica y los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como los niveles de riesgo para los derechos y libertades de las personas físicas, aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado, especialmente en lo relativo al tratamiento de las categorías de datos personales a las que se refiere el artículo 13. En particular, deberán aplicar a los tratamientos de datos personales las medidas incluidas en el Esquema Nacional de Seguridad.*
>
> *2. Por lo que respecta al tratamiento automatizado, el responsable o encargado del tratamiento, a raíz de una evaluación de los riesgos, pondrá en práctica medidas de control con el siguiente propósito:*
>
> *a) En el control de acceso a los equipamientos, denegar el acceso a personas no autorizadas a los equipamientos utilizados para el tratamiento.*
>
> *b) En el control de los soportes de datos, impedir que éstos puedan ser leídos, copiados, modificados o cancelados por personas no autorizadas.*
>
> *c) En el control del almacenamiento, impedir que se introduzcan sin autorización datos personales, o que éstos puedan inspeccionarse, modificarse o suprimirse sin autorización.*
>
> *d) En el control de los usuarios, impedir que los sistemas de tratamiento automatizado puedan ser utilizados por personas no autorizadas por medio de instalaciones de transmisión de datos.*
>
> *e) En el control del acceso a los datos, garantizar que las personas autorizadas a utilizar un sistema de tratamiento automatizado, sólo puedan tener acceso a los datos personales para los que han sido autorizados.*
>
> *f) En el control de la transmisión, garantizar que sea posible verificar y establecer a qué organismos se han transmitido o pueden transmitirse, o a cuya disposición pueden ponerse los datos personales mediante equipamientos de comunicación de datos.*
>
> *g) En el control de la introducción, garantizar que pueda verificarse y constatarse, a posteriori, qué datos personales se han introducido en los*

sistemas de tratamiento automatizado, en qué momento y quién los ha introducido.

h) En el control del transporte, impedir que durante las transferencias de datos personales o durante el transporte de soportes de datos, los datos personales puedan ser leídos, copiados, modificados o suprimidos sin autorización.

i) En el control de restablecimiento, garantizar que los sistemas instalados puedan restablecerse en caso de interrupción.

j) En el control de fiabilidad e integridad, garantizar que las funciones del sistema no presenten defectos, que los errores de funcionamiento sean señalados y que los datos personales almacenados no se degraden por fallos de funcionamiento del sistema.»

Complementariamente a estas medidas se incide de nuevo en la necesidad de establecer un ROP (art.33 de la LOPDP) de modo que se facilite tanto la función de los responsables del tratamiento como de las autoridades de control.

En cuanto al principio de privacidad por diseño y por defecto, recogido en el artículo 28 de la LOPDP lleva aparejado principalmente dos actuaciones: La primera, la privacidad por diseño[94], que consistiría en las actuaciones derivadas de la suma integral del enfoque de riesgo y la responsabilidad proactiva para que el responsable se preocupe de la privacidad desde las fases iniciales de desarrollo y en todo el ciclo de vida de los datos sea el que sea el sistema que los soporte y la segunda, la protección de datos por defecto, que sería la actuación que aplicaría las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento; asimismo que se aplique a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su período de conservación y a su accesibilidad. En concreto, las medidas del responsable garantizarán que, por defecto, los datos personales no sean accesibles, sin intervención de un operador, a un número indeterminado de personas físicas.

2. Legitimación del tratamiento

Hasta la aparición del RGPD y la DDP, la base legal que legitimaba los tratamientos de datos personales en nuestro país era el contenido de la LOPD y ésta, principalmente, fundamentaba la legalidad de los mismos en el consentimiento del interesado.

Es decir, el derecho de autodeterminación informativa se implantaba principalmente en base a la decisión unilateral del interesado. De hecho, el artículo 6 de la ley 15/1999, de 13 de diciembre, disponía que:

«1. El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa.

2. No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones

[94] https://www.aepd.es/sites/default/files/2019-11/guia-privacidad-desde-diseno.pdf

públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6, de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado.

3. El consentimiento a que se refiere el artículo podrá ser revocado cuando exista causa justificada para ello y no se le atribuyan efectos retroactivos.

4. En los casos en los que no sea necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal, y siempre que una ley no disponga lo contrario, éste podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En tal supuesto, el responsable del fichero excluirá del tratamiento los datos relativos al afectado.»

En cuanto a la categoría especiales de datos personales (antiguos datos especialmente protegidos) los artículos 7 y 8 volvían a girar en torno al consentimiento, está vez, un poco más informado, de modo que se obligaba en todo caso a que fuera expreso y por escrito.[95]

---

[95] Artículo 7. *«Datos especialmente protegidos. 1. De acuerdo con lo establecido en el apartado 2 del artículo 16 de la Constitución, nadie podrá ser obligado a declarar sobre su ideología, religión o creencias. Cuando en relación con estos datos se proceda a recabar el consentimiento a que se refiere el apartado siguiente, se advertirá al interesado acerca de su derecho a no prestarlo. 2. Sólo con el consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias. Se exceptúan los ficheros mantenidos por los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, en cuanto a los datos relativos a sus asociados o miembros, sin perjuicio de que la cesión de dichos datos precisará siempre el previo consentimiento del afectado. 3. Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente. 4. Quedan prohibidos los ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico, o vida sexual. 5. Los datos de carácter personal relativos a la comisión de infracciones penales o administrativas sólo podrán ser incluidos en ficheros de las Administraciones públicas competentes en los supuestos previstos en las respectivas normas reguladoras. 6. No obstante lo dispuesto en los apartados anteriores, podrán ser objeto de tratamiento los datos de carácter personal a que se refieren los apartados 2 y 3 de este artículo, cuando dicho tratamiento resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto. También podrán ser objeto de tratamiento los datos a que se refiere el párrafo anterior cuando el tratamiento sea necesario para salvaguardar el interés vital del afectado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento. Artículo 8. Datos relativos a la salud. Sin perjuicio de lo que se dispone en el artículo 11 respecto de la cesión, las instituciones y los centros sanitarios públicos y privados y los profesionales correspondientes podrán proceder al tratamiento de los datos de carácter personal relativos a la salud de las personas que a ellos acudan o hayan de ser tratados en los mismos, de acuerdo con lo dispuesto en la legislación estatal o autonómica sobre sanidad.»*

La previsión recogida en el apartado primero de este artículo quedaba explicada en el artículo 10.1 del 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 que incidía en que:

«1. Los datos de carácter personal únicamente podrán ser objeto de tratamiento o cesión si el interesado hubiera prestado previamente su consentimiento para ello.»

Si bien, ya este RLOPD venía a desarrollar y adaptar el contenido del apartado 2 del precitado artículo 6 de la LOPD. De este modo, enumeraba algunas de las excepciones legales al consentimiento indicando que era posible el tratamiento y la cesión de datos personales sin necesidad del mismo, cuando:

- Se recogieran para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de las competencias que les atribuya una norma con rango de ley o una norma de derecho comunitario.
- Se recabasen por el responsable del tratamiento con ocasión de la celebración de un contrato o precontrato o de la existencia de una relación negocial, laboral o administrativa de la que sea parte el afectado y sean necesarios para su mantenimiento o cumplimiento.
- El tratamiento de los datos tuviese por finalidad proteger un interés vital del interesado

De la misma manera amparaba la cesión sin consentimiento cuando:

- La cesión respondiera a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control comporte la comunicación de los datos. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.
- La comunicación que debiera efectuarse tuviera por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas o a las instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas y se realice en el ámbito de las funciones que la ley les atribuya expresamente.
- La cesión entre Administraciones públicas cuando concurriera uno de los siguientes supuestos:
  - Tener por objeto el tratamiento de los datos con fines históricos, estadísticos o científicos.
  - Los datos de carácter personal hayan sido recogidos o elaborados por una Administración pública con destino a otra.
  - La comunicación se realice para el ejercicio de competencias idénticas o que versen sobre las mismas materias[96].

[96] En este aspecto resulta fundamental la Sentencia del Tribunal Constitucional nº 17/2013 de 31 de enero, que determinan aquellos supuestos y garantías que han de observarse en la comunicación de datos entre administraciones públicas: *«Tal y como ha sido interpretado por el TC en dicha sentencia, este precepto se refiere a la cesión no consentida de los datos relativos a la residencia o el domicilio a otras Administraciones públicas que así lo soliciten solamente en aquellos casos en los que, para el ejercicio de sus competencias, sean aquellos datos relevantes»; «El TC*

En cuanto a las categorías especiales de datos (antiguos datos especialmente protegidos) el RLOPD enmarcaba en el contenido de los artículos 7 y 8 de la LOPD con la singularidad de determinar que no era necesario consentir para la comunicación de datos personales sobre la salud, incluso a través de medios electrónicos, entre organismos, centros y servicios del Sistema Nacional de Salud cuando se realizase para la atención sanitaria de las personas, conforme a lo dispuesto en el Capítulo V de la Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud.

Con respecto al tratamiento de los datos por parte de las Fuerzas y Cuerpos de Seguridad, el sistema que hoy viene regulado por varias leyes orgánicas, en esta LOPD, venía establecido principalmente por el contenido de unos pocos artículos cuya interpretación ha sido causa de cierta controversia a la hora de que estos organismos pudieran cumplir con sus misiones en base a la idea antes señalada de utilizar la normativa de protección de datos personales como una traba o un impedimento a la hora de facilitarles el acceso o cederles los datos.

El artículo 2.3 de la LOPD excluía de su ámbito de aplicación los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada. No obstante, en estos supuestos el responsable del fichero comunicaba previamente la existencia del mismo, sus características generales y su finalidad a la Agencia de Protección de Datos e, igualmente, el artículo 3, apartado e) hacía una remisión a la normativa específica aplicable con subsidiariedad propia de dicha Ley Orgánica a los procedentes de imágenes y sonidos obtenidos mediante la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad, de conformidad con la legislación sobre la materia.

Tras ello, como ficheros de titularidad pública, obligaba a los ficheros con finalidad *«policial»* a que su creación, modificación o supresión sólo pudiera hacerse por medio de disposición general publicada en el «Boletín Oficial del Estado» o Diario oficial correspondiente y establecía sus especificaciones en los artículos 22 a 24 que se recogen a continuación:

> *«Artículo 22. Ficheros de las Fuerzas y Cuerpos de Seguridad.*
>
> *1. Los ficheros creados por las Fuerzas y Cuerpos de Seguridad que contengan datos de carácter personal que, por haberse recogido para fines administrativos, deban ser objeto de registro permanente, estarán sujetos al régimen general de la presente Ley.*
>
> *2. La recogida y tratamiento para fines policiales de datos de carácter personal por las Fuerzas y Cuerpos de Seguridad sin consentimiento de las personas afectadas están limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales, debiendo ser almace-*

ha determinado que (i) habrá de evitarse el acceso indiscriminado y masivo a los datos personales (ii) el dato en cuestión solicitado habrá de ser pertinente y necesario (iii) para la finalidad establecida en el precepto (iv) la solicitud de acceso a los concretos datos personales habrá de motivarse y justificarse expresamente, (v) de manera que ello posibilite su control por el cedente (vi) y se evite un uso torticero de esa facultad con accesos masivos. Ello supone (vii) que ha de quedar garantizada la posibilidad de analizar si en cada caso concreto el acceso tenía amparo en lo establecido en la ley (art. 16.3 LBRL)

nados en ficheros específicos establecidos al efecto, que deberán clasificarse por categorías en función de su grado de fiabilidad.

3. La recogida y tratamiento por las Fuerzas y Cuerpos de Seguridad de los datos, a que hacen referencia los apartados 2 y 3 del artículo 7, podrán realizarse exclusivamente en los supuestos en que sea absolutamente necesario para los fines de una investigación concreta, sin perjuicio del control de legalidad de la actuación administrativa o de la obligación de resolver las pretensiones formuladas en su caso por los interesados que corresponden a los órganos jurisdiccionales.

4. Los datos personales registrados con fines policiales se cancelarán cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento.

A estos efectos, se considerará especialmente la edad del afectado y el carácter de los datos almacenados, la necesidad de mantener los datos hasta la conclusión de una investigación o procedimiento concreto, la resolución judicial firme, en especial la absolutoria, el indulto, la rehabilitación y la prescripción de responsabilidad.

Artículo 23. Excepciones a los derechos de acceso, rectificación y cancelación.

1. Los responsables de los ficheros que contengan los datos a que se refieren los apartados 2, 3 y 4 del artículo anterior podrán denegar el acceso, la rectificación o cancelación en función de los peligros que pudieran derivarse para la defensa del Estado o la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que se estén realizando.

2. Los responsables de los ficheros de la Hacienda Pública podrán, igualmente, denegar el ejercicio de los derechos a que se refiere el apartado anterior cuando el mismo obstaculice las actuaciones administrativas tendentes a asegurar el cumplimiento de las obligaciones tributarias y, en todo caso, cuando el afectado esté siendo objeto de actuaciones inspectoras.

3. El afectado al que se deniegue, total o parcialmente, el ejercicio de los derechos mencionados en los apartados anteriores podrá ponerlo en conocimiento del Director de la Agencia de Protección de Datos o del organismo competente de cada Comunidad Autónoma en el caso de ficheros mantenidos por Cuerpos de Policía propios de éstas, o por las Administraciones tributarias autonómicas, quienes deberán asegurarse de la procedencia o improcedencia de la denegación.

Artículo 24. Otras excepciones a los derechos de los afectados.

1. Lo dispuesto en los apartados 1 y 2 del artículo 5 no será aplicable a la recogida de datos cuando la información al afectado impida o dificulte gravemente el cumplimiento de las funciones de control y verificación de las Administraciones públicas o cuando afecte a la Defensa Nacional, a la seguridad pública o a la persecución de infracciones penales o administrativas.»

En el RLOPD sólo se hablaba de ficheros policiales a la hora de aplicar los niveles de seguridad a los ficheros que contuvieran o se refirieran a datos recabados para fines policiales sin consentimiento de las personas afectadas

Como puede apreciarse era un sistema que obligaba a acoger el régimen general para los ficheros que tuvieran finalidades administrativas (se basaran o no en el consentimiento de la persona interesada) pero que, para los tratamientos

con fines propiamente policiales de prevención, detección o investigación de delitos, albergaba enormes lagunas que fueron completándose con algunos informes de la AEPD, la Jurisprudencia y con la labor constante y encomiable de los miembros de las FCS a la hora de aplicar e interpretar en primera instancia los presupuestos legales.

Tras el establecimiento del RGPD, puede asegurarse que el sistema basando en el *«cosentimientocentrismo»* cambio de modo que pasó de ser la base principal en la que se basaba la normativa, a ser una causa más de legitimación entre otras causas que justifican y amparan el tratamiento de los datos.

Este Reglamento, en la actualidad, recoge estas seis condiciones para su licitud. Consisten en que:

- el interesado de su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;
- el tratamiento sea necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;
- el tratamiento sea necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;
- el tratamiento resulte necesario para proteger intereses vitales del interesado o de otra persona física;
- el tratamiento resulte necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;
- el tratamiento resulte necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.

En el caso de los tratamientos con finalidad policial, tal y como se apuntaba con carácter previo, el consentimiento del interesado no constituye un fundamento jurídico para el tratamiento de los datos personales por las autoridades competentes ya que cuando se exige al interesado que cumpla una obligación jurídica, este no goza de verdadera libertad de elección, por lo que no puede considerarse que su respuesta constituya una manifestación libre de su voluntad.

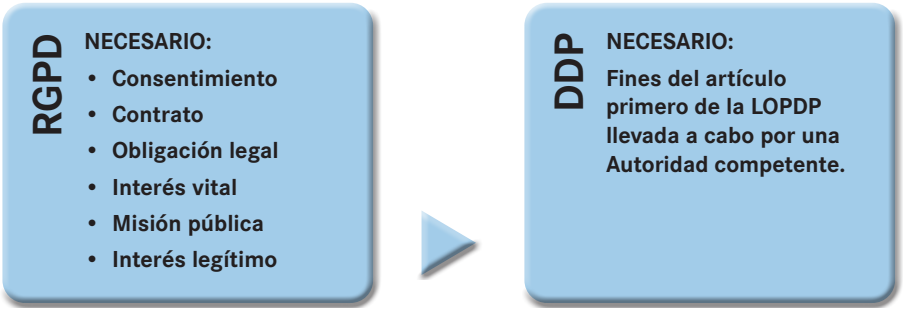
Ello no debe ser óbice para que se establezca legalmente la posibilidad de que el interesado pueda aceptar el tratamiento de sus datos personales a los efectos de la DDP, por ejemplo, para el control del paradero del interesado mediante dispositivos electrónicos para la ejecución de sanciones penales.

Si bien, ese acto es para consentir la actuación no para legitimar el tratamiento posterior de sus datos.

Por tanto, la única base de legitimación necesaria en este ámbito «policial» es que el tratamiento sea lícito en la medida en que sea necesario para los fines de prevención, detección, investigación y enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y prevención frente a las

amenazas contra la seguridad pública y se realice por una autoridad competente en ejercicio de sus funciones.

Desde un punto de vista descriptivo se puede observar en el siguiente gráfico:



La necesidad, como vemos, cobra una especial relevancia en todos los tratamientos de datos personales. Esta circunstancia implicaría el requerimiento de una evaluación combinada, basada en hechos, sobre la eficacia de la medida para el objetivo perseguido y sobre si resulta menos intrusiva en comparación con otras opciones para lograr el mismo objetivo.

Según el *«Manual para la evaluación de la necesidad de las medidas que limiten el derecho fundamental a la protección de datos de carácter personal»*, del Supervisor Europeo de Protección de Datos, la necesidad se constituye en: «...(...) *un principio de calidad de los datos y una condición recurrente en casi todos los requisitos sobre la legalidad del tratamiento de los datos de carácter personal que se derivan de la legalidad derivada de la protección de datos de la UE. También existe un vínculo entre el apartado 2 del artículo 8 de la Carta y el derecho derivado, ya que el apartado 2 del artículo 8 hace referencia al fundamento legítimo para el tratamiento "previsto por la ley" y la nota explicativa del artículo 8 hace referencia a este derecho derivado afirmando que la Directiva 95/46 y el Reglamento 45/2001 "contienen condiciones y limitaciones para el ejercicio del derecho a la protección de los datos de carácter personal".»*

V. TRATAMIENTO DE DATOS DE MENORES, PERSONAS CON DISCAPACIDAD Y FALLECIDOS

1. Menores de edad

Como se ha apuntado, el consentimiento no es una base legitimadora del tratamiento con fines policiales, si bien, los datos de los menores de edad están dotados de un grado de protección que hace necesario cumplir con una serie de requisitos (sobre todo de seguridad y protección de los datos) que los pueden incluir en una subcategoría de los susodichos datos de categoria especial a tener en cuenta.

Según el *«Documento de trabajo 1/08 sobre la protección de datos personales de los niños»*, de 18 de febrero de 2008, del WP29, se ha define como «niño» (de conformidad con los criterios de los instrumentos internacionales más importantes), como una persona natural con menos de 18 años, a menos que se haya emancipado legalmente antes de dicha edad.

En el RGPD se utiliza indistintamente el término *«niño»* o *«menor de edad»* por lo que con arreglo a nuestra legislación española, el significado será el mismo pues está refiriéndose a los menores de 18 años

En la legislación europea sobre protección de datos no se había regulado hasta el momento la cuestión particular de la protección de datos de los menores. Así, resulta oportuno apuntar que esta cuestión no se recogió en la Directiva 95/46/CE, ni en la Directiva 2002/58/CE, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (así como, en la modificación por la Directiva 2009/136/CE).

Si bien, aunque en nuestra LOPD no se hacía mención a este supuesto, en el RLPOD sí encontrábamos en el artículo 13, un precepto dedicado al consentimiento de los menores de edad cuyo contenido se reproduce:

> *«Artículo 13. Consentimiento para el tratamiento de datos de menores de edad.*
>
> *1. Podrá procederse al tratamiento de los datos de los mayores de catorce años con su consentimiento, salvo en aquellos casos en los que la Ley exija para su prestación la asistencia de los titulares de la patria potestad o tutela. En el caso de los menores de catorce años se requerirá el consentimiento de los padres o tutores.*
>
> *2. En ningún caso podrán recabarse del menor datos que permitan obtener información sobre los demás miembros del grupo familiar, o sobre las características del mismo, como los datos relativos a la actividad profesional de los progenitores, información económica, datos sociológicos o cualesquiera otros, sin el consentimiento de los titulares de tales datos. No obstante, podrán recabarse los datos de identidad y dirección del padre, madre o tutor con la única finalidad de recabar la autorización prevista en el apartado anterior.*
>
> *3. Cuando el tratamiento se refiera a datos de menores de edad, la información dirigida a los mismos deberá expresarse en un lenguaje que sea fácilmente comprensible por aquéllos, con expresa indicación de lo dispuesto en este artículo.*
>
> *4. Corresponderá al responsable del fichero o tratamiento articular los procedimientos que garanticen que se ha comprobado de modo efectivo la*

edad del menor y la autenticidad del consentimiento prestado en su caso, por los padres, tutores o representantes legales.»

Como puede observarse, se instituyó un sistema basado igualmente en el consentimiento del menor o sus re*presentantes legales (salvo obligación legal), con la* particularidad de que se exigía del responsable de fichero la comprobación efectiva tanto de la edad como del consentimiento prestado por éstos.

En el citado *«Documento de trabajo 1/08 GT29 sobre la protección de datos personales de los niños»*, se recogían unos principios y derechos relativos a la protección de datos y unas políticas de actuación que se pueden resumir en los siete apartados siguientes:

(1) Interés superior del niño. La base de este principio es que una persona que aún no ha alcanzado la madurez física y psicológica necesita más protección que otros (2) Protección y cuidado necesario para el bienestar de los niños. En primer lugar, la inmadurez del niño le hace vulnerable y ello debe compensarse mediante una protección y cuidados adecuados. En segundo lugar, el derecho del niño al desarrollo sólo puede disfrutarse adecuadamente con la asistencia o protección de otras entidades y/o personas

(3) Derecho a la intimidad. Como ser humano, el niño tiene derecho a la intimidad

(4) Representación. Los niños, por ser menores de edad, tienen limitada su capacidad de obrar. Por tal motivo muchas de sus actuaciones deben ser realizadas por quienes ostentan su representación legal

(5) Intereses en conflicto intimidad y el interés superior del niño. El principio exige que se proteja la intimidad del niño del mejor modo posible

(6) Adaptación al grado de madurez del niño. Puesto que el niño es una persona todavía en desarrollo, el ejercicio de sus derechos (incluyendo los relativos a la protección de datos) debe adaptarse a su nivel de desarrollo físico y psicológico

(7) Derecho a ser consultado. De manera gradual, los niños van siendo capaces de contribuir a la toma de decisiones que les afectan.

En nuestra normativa interna principalmente se señalan las siguientes cuestiones relacionadas con la protección de los datos personales de menores de edad:

- La Ley Orgánica 1/1982 de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen en su artículo tercero dispone que los menores e incapaces deberán prestar el consentimiento por ellos mismos si su condición de madurez lo permite de acuerdo con la legislación civil. En los restantes casos, el consentimiento habrá de otorgarse mediante escrito por su representante legal, quien estará obligado a poner en conocimiento previo del Ministerio Fiscal el consentimiento proyectado. Si en el plazo de ocho días el Ministerio Fiscal se opusiere, resolverá el Juez.
- El art. 162.1 del Código Civil, dice que los padres que ostenten la patria potestad tienen la representación legal de sus hijos menores no emancipados, exceptuando, los actos relativos a derechos de la personalidad u otros

que el hijo, de acuerdo con las leyes y con sus condiciones de madurez, pueda realizar por sí mismo.

- El art 7.5 de la referida Ley Orgánica 1/1982, indica que tendrán la consideración de intromisiones ilegítimas en el ámbito de protección delimitado por el artículo 2 de esta ley, la captación, reproducción o publicación por fotografía, filme o cualquier otro procedimiento, de la imagen de una persona en lugares o momentos de su vida privada o fuera de ellos.
- Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor, de modificación parcial del Código Civil y de la Ley de Enjuiciamiento Civil recoge en su artículo 4 que los menores tienen derecho al honor, a la intimidad personal y familiar y a la propia imagen. Este derecho comprende también la inviolabilidad del domicilio familiar y de la correspondencia, así como del secreto de las comunicaciones.

Del mismo modo fija que, la difusión de información o la utilización de imágenes o nombre de los menores en los medios de comunicación que puedan implicar una intromisión ilegítima en su intimidad, honra o reputación, o que sea contraria a sus intereses, determinará la intervención del Ministerio Fiscal[97], que solicitará de inmediato las medidas cautelares y de protección previstas en la Ley y solicitará las indemnizaciones que correspondan por los perjuicios causados.

Considerando intromisión ilegítima en el derecho al honor, a la intimidad personal y familiar y a la propia imagen del menor, cualquier utilización de su imagen o su nombre en los medios de comunicación que pueda implicar menoscabo de su honra o reputación, o que sea contraria a sus intereses incluso si consta el consentimiento del menor o de sus representantes legales.

Sin perjuicio de las acciones de las que sean titulares los representantes legales del menor, corresponde en todo caso al Ministerio Fiscal su ejercicio, que podrá actuar de oficio o a instancia del propio menor o de cualquier persona interesada, física, jurídica o entidad pública y los padres o tutores y los poderes públicos respetarán estos derechos y los protegerán frente a posibles ataques de terceros.

La Ley Orgánica del año 1996, específica en su artículo 22 quáter, para el caso de situaciones de desprotección del menor que:

> *«1. Para el cumplimiento de las finalidades previstas en el capítulo I del título II de esta ley, las Administraciones Públicas competentes podrán proceder, sin el consentimiento del interesado, a la recogida y tratamiento de los datos que resulten necesarios para valorar la situación del menor, incluyendo tanto los relativos al mismo como los relacionados con su entorno familiar o social.*
>
> *Los profesionales, las Entidades Públicas y privadas y, en general, cualquier persona facilitarán a las Administraciones Públicas los informes y antecedentes sobre los menores, sus progenitores, tutores, guardadores o acogedo-*

[97] Instrucción 2/2006, de 15 de marzo, sobre el Fiscal y la protección del derecho al honor, intimidad y propia imagen de los menores y la Instrucción 1/2017, de 27 de marzo, sobre la actuación del fiscal para la protección de los derechos al honor, intimidad y propia imagen de menores de edad con discapacidad ante los medios de comunicación audiovisual.

res, que les sean requeridos por ser necesarios para este fin, sin precisar del consentimiento del afectado.

2. Las entidades a las que se refiere el artículo 13 podrán tratar sin consentimiento del interesado la información que resulte imprescindible para el cumplimiento de las obligaciones establecidas en dicho precepto con la única finalidad de poner dichos datos en conocimiento de las Administraciones Públicas competentes o del Ministerio Fiscal.

3. Los datos recabados por las Administraciones Públicas podrán utilizarse única y exclusivamente para la adopción de las medidas de protección establecidas en la presente ley, atendiendo en todo caso a la garantía del interés superior del menor y sólo podrán ser comunicados a las Administraciones Públicas que hubieran de adoptar las resoluciones correspondientes, al Ministerio Fiscal y a los órganos judiciales.

4. Los datos podrán ser igualmente cedidos sin consentimiento del interesado al Ministerio Fiscal, que los tratará para el ejercicio de las funciones establecidas en esta ley y en la normativa que le es aplicable.

5. En todo caso, el tratamiento de los mencionados datos quedará sometido a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y sus disposiciones de desarrollo, siendo exigible la implantación de las medidas de seguridad de nivel alto previstas en dicha normativa.»

A nivel estrictamente de las FCS, en concreto las FCSE la Instrucción 1/2007, de la Secretaría de Estado de Seguridad, por la que se actualiza el *«Protocolo de Actuación Policial con Menores»* incluye varias previsiones en cuanto al tratamiento de datos de menores:

En cuanto a la publicidad de las actuaciones establece que no se permitirá que se obtengan o difundan imágenes del menor, sea autor o testigo de una infracción penal, ni se facilitarán datos que permitan su identificación, con pleno cumplimiento de las normas relativas a la protección jurídica de menores, especialmente el derecho al honor, a la intimidad, a la propia imagen y a la protección de la juventud y de la infancia y establece la prohibición, en todo caso, la divulgación o publicación sin la correspondiente autorización de información relativa a la identidad de víctimas menores de edad, de datos que puedan facilitar su identificación de forma directa o indirecta, o de aquellas circunstancias personales que hubieran sido valoradas para resolver sobre sus necesidades de protección, así como la obtención, divulgación o publicación de imágenes suyas o de sus familiares.

También incluye previsiones para el caso de menores desaparecidos y contiene un apartado específico relativo a los registros policiales de datos de menores que es importante reproducir en esta obra y observar cuáles serán las modificaciones que hay que interpretar en base a la entrada en vigor del RGPD, la LOPDGDD[98] de la LOPDP:

[98] De hecho los ficheros ADEXTRA se ha adaptado a la normativa y está publicitado en el RAT del Ministerio del Interior con las siguientes previsiones en cuanto al tratamiento de datos de menores: *«De menores indocumentados o en situación legal de desamparo: Nombre y apellidos, fecha y lugar de nacimiento, sexo, nacionalidad, domicilio, centro de acogida o lugar de residencia, teléfono, última residencia en el país de procedencia, impresiones dactilares, fotografía, Organismo*

«10. REGISTROS POLICIALES DE DATOS PERSONALES DE MENORES

10.1. Acceso y confidencialidad de los registros

10.1.1. Los registros policiales donde conste la identidad y otros datos que afecten a la intimidad de los menores serán de carácter estrictamente confidencial y no podrán ser consultados por terceros, distinguiéndose tres tipos en función del soporte:

a. Libros-registro, en soporte papel.

b. Bases de datos, en soporte informático.

c. Álbumes fotográficos, colección de fotografías.

10.1.2. Sólo tendrán acceso a estos registros las personas que participen directamente en la investigación de un caso en trámite o que, en ejercicio de sus competencias, sean expresamente autorizados para ello por el Juez de Menores o el Fiscal de la Sección de Menores.

10.2. Libros-Registros

10.2.1. El Libro-Registro de Menores Detenidos está regulado en la Instrucción 7/2005, de 25 de abril, de la Secretaría de Estado de Seguridad, debiendo tenerse en cuenta que:

a. Se anotarán las incidencias que puedan producirse en las dependencias policiales durante la permanencia en las mismas de menores entre catorce y dieciocho años, presuntamente responsables de la comisión de infracciones penales.

b. Tendrá carácter confidencial y será único para todo lo concerniente al menor, no consignándose sus datos en el Libro de Registro y Custodia de Detenidos ni en ningún otro libro de la dependencia policial.

c. Los datos de este registro estarán exclusivamente a disposición del Ministerio Fiscal y de la Autoridad Judicial competente.

10.2.2. En el Libro-Registro de actuaciones con Menores e Incapaces en Situaciones de Riesgo, regulado en la Instrucción 2/2001, de 4 de julio, de la Secretaría de Estado de Seguridad, se anotarán las actuaciones policiales que impliquen el paso o la estancia obligada en dependencias policiales o la limitación de la libertad ambulatoria de los menores o incapaces en situaciones de riesgo con finalidad de protección:

a. Menores de edad inferior a catorce años presuntamente responsables de la comisión de infracciones penales.

b. Menores de dieciocho años en situación de riesgo o desamparo, incluyendo los fugados del domicilio familiar o institucional y los desaparecidos por distintas causas.

c. Personas con discapacidad intelectual necesitadas de especial protección, sean mayores o menores de edad.

10.2.3. En el Libro-Registro de Diligencias de Identificación, conforme a lo dispuesto en el artículo 16 de la Ley Orgánica 4/2015, de 30 de marzo, y a lo dispuesto en la instrucción quinta, apartado 4, de la Instrucción 7/2015 de la Secretaria de Estado de Seguridad, de 30 de junio, "relativa a la práctica de diligencias de identificación de registros corporales externos y actuaciones con menores", se harán constar las diligencias de identificación realizadas en

---

Público bajo cuya protección se halle, informe médico forense de resultado de la prueba ósea de determinación de la edad, marcas y deficiencias físicas y psíquicas, tatuajes, características físicas o antropométricas, situación de indocumentado o de situación legal de desamparo; nombre, apellidos y domicilio de los padres, tutores o guardadores y cualquier otro dato de relevancia a los citados efectos identificadores.»

dependencias oficiales de las Fuerzas y Cuerpos de Seguridad, estando en todo momento a disposición de la Autoridad Judicial competente y del Ministerio Fiscal.

10.2.4. En el ámbito de la Inspección de Personal y Servicios de Seguridad (IPSS) de la Secretaría de Estado de Seguridad se encuentra en desarrollo un proyecto de digitalización y estandarización del contenido de los libros de registro de la Secretaría de Estado de Seguridad, que incluirá los relativos a actuaciones con menores de edad enumerados en los apartados anteriores.

10.3. Bases de datos

10.3.1. Existirá una aplicación específica donde se registrarán los datos correspondientes a menores entre catorce y dieciocho años encartados en una investigación policial.

10.3.2. Las detenciones de menores infractores entre catorce y dieciocho años quedarán registradas en una aplicación específica donde consten los antecedentes policiales de menores.

10.3.3. Todas las reseñas policiales de menores quedarán contenidas en su correspondiente aplicación, debiendo mantener separadas y sin comunicación directa las reseñas de menores detenidos de aquellas otras practicadas con ocasión de trámites de determinación de edad o de identificación de menores no acompañados o indocumentados.

10.3.4. Se registrarán las requisitorias emitidas por Autoridades Fiscales y Judiciales que contemplen cualquier interés sobre un menor de dieciocho años, tanto en materia de protección como de reforma, y las requisitorias emitidas por otras Autoridades competentes, principalmente policiales y de protección de menores, referentes a la búsqueda y localización de menores de dieciocho años. El acceso a esta información deberá estar disponible para cualquier unidad policial, a las personas que participen directamente en la investigación, con un adecuado control que permita supervisar las consultas.

10.3.5. El Registro de Menores Extranjeros No Acompañados (RMENA) está ubicado en el subfichero de la aplicación ADEXTRA cuya titularidad corresponde a la Dirección General de la Policía, y su gestión a la Comisaría General de Extranjería y Fronteras. Se trata de un registro de naturaleza administrativa a efectos exclusivos de identificación, regulado en el artículo 215 del Real Decreto 557/2011, de 20 de abril, por el que se aprueba el Reglamento de la Ley Orgánica 4/2000, de 11 de enero, sobre derechos y libertades de los extranjeros en España. El Registro contiene los datos personales referentes a la identificación de todos los menores extranjeros no acompañados, documentados e indocumentados, cuya minoría de edad resulte indubitada desde el momento de su localización o haya sido determinada por Decreto del Ministerio Fiscal.

10.4. Álbumes fotográficos

10.4.1. La confección y tenencia de álbumes fotográficos de menores detenidos, tanto en soporte físico como digital, corresponderá a los Grupos o Equipos especializados en el tratamiento policial de menores y, en su caso, a las Unidades de investigación en esta materia.

10.4.2. Estos álbumes sólo contendrán la fotografía de aquellos menores infractores entre catorce y dieciocho años detenidos por delitos.

10.4.3. Para su confección se seguirá un criterio restrictivo basado en la edad, especialmente entre dieciséis y dieciocho años, habitualidad o reincidencia delictiva del menor, así como en la comisión de hechos delictivos de carácter violento, sexual o terrorista.

10.4.4. El uso de estas colecciones estará restringido a los solos fines de identificación e investigación policial.»

Es importe señalar que ninguna de las disposiciones apuntadas prohíbe el tratamiento de datos de menores de edad, si bien imponen una serie de requisitos específicos para su protección que deben ser tenidos en cuenta por los posibles responsables del tratamiento para garantizar la seguridad de éstos.

En su considerando 38, el RGPD enuncia que *«los niños merecen una protección específica de sus datos personales, ya que pueden ser menos conscientes de los riesgos, consecuencias, garantías y derechos concernientes al tratamiento de datos personales. Dicha protección específica debe aplicarse en particular, a la utilización de datos personales de niños con fines de mercadotecnia o elaboración de perfiles de personalidad o de usuario, y a la obtención de datos personales relativos a niños cuando se utilicen servicios ofrecidos directamente a un niño. El consentimiento del titular de la patria potestad o tutela no debe ser necesario en el contexto de los servicios preventivos o de asesoramiento ofrecidos directamente a los niños.»*

De la misma manera, en el 58 dispone que, dado que los niños merecen una protección específica, cualquier información y comunicación cuyo tratamiento les afecte debe facilitarse en un lenguaje claro y sencillo que sea fácil de entender.

En el artículo 8, además de exigir que se cumplan los principios generales de tratamiento, detalla una especificación en relación con el consentimiento de los menores en las actuaciones relativas a los servicios de la sociedad de la información:

«1. Cuando se aplique el artículo 6, apartado 1, letra a), en relación con la oferta directa a niños de servicios de la sociedad de la información, el tratamiento de los datos personales de un niño se considerará lícito cuando tenga como mínimo 16 años. Si el niño es menor de 16 años, tal tratamiento únicamente se considerará lícito si el consentimiento lo dio o autorizó el titular de la patria potestad o tutela sobre el niño, y solo en la medida en que se dio o autorizó. Los Estados miembros podrán establecer por ley una edad inferior a tales fines, siempre que esta no sea inferior a 13 años.

2. El responsable del tratamiento hará esfuerzos razonables para verificar en tales casos que el consentimiento fue dado o autorizado por el titular de la patria potestad o tutela sobre el niño, teniendo en cuenta la tecnología disponible. 3. El apartado 1 no afectará a las disposiciones generales del derecho contractual de los Estados miembros, como las normas relativas a la validez, formación o efectos de los contratos en relación con un niño.»

Sin olvidar que, este instrumento, establece asimismo los requisitos que deben cumplirse en el caso de que los datos se traten con otras finalidades como las científicas o investigadoras (Vid. arts. 5.1 b) y 89)

Como puede verse, en opinión de los autores, las medidas son más laxas que las que se exigían en la LOPD ya que no establece claramente una obligación de verificar la edad y solo impone los esfuerzos que sean razonables para acreditar el consentimiento (lo cual es reseñable y digno de un profundo análisis por quién corresponda)

La LOPDGDD, adapta la cuestión del consentimiento de los menores en su artículo 7[99] ampliando dicha previsión a cualquier supuesto en el que sea necesario el consentimiento sin perjuicio de las distintas normativas específicas donde se pueden ver involucrados, afectados o interesados los menores. Por lo que sería obvio entender que permite los tratamientos que no se justifiquen en esa base de legitimación.

Como puede verse, en los supuestos concretos de legitimación por consentimiento, éste se permite a los mayores de 14 años salvo que la ley no habilite personalmente al menor a prestarlo en base el tratamiento singular que se realice. Para el supuesto de los menores de 14 años se demanda en todo caso la habilitación de las actuaciones en base al consentimiento de los representantes legales (salvo, claro está, que los supuestos en los participen no lo demanden o lo hagan perjudicando al menor. Pensemos en casos en material civil donde los intereses del menor los proteja el Ministerio Fiscal o el organismo competente y sus pretensiones serán contrarias a las de sus progenitores o similares.)

La LOPDP los categoriza como una categoría especial en su artículo 13.3 determinando una única premisa: *«que datos de los menores de edad y de las personas con capacidad modificada judicialmente o que estén incursas en procesos de dicha naturaleza, se tratarán garantizando el interés superior de los mismos y con el nivel de seguridad adecuado.»*

Por lo tanto, dentro del ámbito policial se puede producir el tratamiento de datos de menores de edad, si bien, deberán adecuarse para garantizar el interés superior del menor y los principios y finalidades del ámbito de aplicación del tratamiento en estos supuestos, elevándose en lo necesario las medidas de protección para garantizar sus derechos.

2. Personas fallecidas y personas con discapacidad

El artículo 32 del Código Civil dispone que: *«La personalidad civil se extingue por la muerte de las personas.»* Por dicho motivo, a partir de ese momento, los seres humanos no pueden ser considerados personas físicas en el sentido del marco de trabajo que nos atañe en este estudio.

Del mismo modo, los artículos 4º, 5º y 6º de la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen disponen respectivamente que:

> *«Artículo cuarto.*
> *Uno. El ejercicio de las acciones de protección civil del honor, la intimidad o la imagen de una persona fallecida corresponde a quien ésta haya designa-*

[99] Artículo 7. *«Consentimiento de los menores de edad. 1. El tratamiento de los datos personales de un menor de edad 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. 2. 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.»*

do a tal efecto en su testamento. La designación puede recaer en una persona jurídica.

Dos. No existiendo designación o habiendo fallecido la persona designada, estarán legitimados para recabar la protección el cónyuge, los descendientes, ascendientes y hermanos de la persona afectada que viviesen al tiempo de su fallecimiento.

Tres. A falta de todos ellos, el ejercicio de las acciones de protección corresponderá al Ministerio Fiscal, que podrá actuar de oficio a instancia de persona interesada, siempre que no hubieren transcurrido más de ochenta años desde el fallecimiento del afectado. El mismo plazo se observará cuando el ejercicio de las acciones mencionadas corresponda a una persona jurídica designada en testamento.

Cuatro. En los supuestos de intromisión ilegítima en los derechos de las víctimas de un delito a que se refiere el apartado ocho del artículo séptimo, estará legitimado para ejercer las acciones de protección el ofendido o perjudicado por el delito cometido, haya o no ejercido la acción penal o civil en el proceso penal precedente. También estará legitimado en todo caso el Ministerio Fiscal. En los supuestos de fallecimiento, se estará a lo dispuesto en los apartados anteriores.

Artículo quinto

Uno. Cuando sobrevivan varios parientes de los señalados en el artículo anterior, cualquiera de ellos podrá ejercer las acciones previstas para la protección de los derechos del fallecido.

Dos. La misma regla se aplicará, salvo disposición en contrario del fallecido, cuando hayan sido varias las personas designadas en su testamento.

Artículo sexto

Uno. Cuando el titular del derecho lesionado fallezca sin haber podido ejercitar por sí o por su representante legal las acciones previstas en esta ley, por las circunstancias en que la lesión se produjo, las referidas acciones podrán ejercitarse por las personas señaladas en el artículo cuarto.

Dos. Las mismas personas podrán continuar la acción ya entablada por el titular del derecho lesionado cuando falleciere.»

El RGPD no se aplica a la protección de datos personales de personas fallecidas (ni siquiera con fines de archivo o investigación histórica), si bien, faculta a los Estados miembros son competentes para establecer normas relativas al tratamiento de sus datos.

En base a esta facultad, la LOPDGDD, tras excluir del ámbito de aplicación de la ley su tratamiento, se permite que las personas vinculadas al fallecido por razones familiares o de hecho o sus herederos puedan solicitar el acceso a los mismos, así como su rectificación o supresión, en su caso con sujeción a las instrucciones del fallecido y por supuesto con sujeción a las condiciones establecidas por el responsable del tratamiento.

En sus artículos 3 y 96 se indica respectivamente lo siguiente:

«Artículo 3. Datos de las personas fallecidas.

1. Las personas vinculadas al fallecido por razones familiares o de hecho así como sus herederos podrán dirigirse al responsable o encargado del tratamiento al objeto de solicitar el acceso a los datos personales de aquella y, en su caso, su rectificación o supresión.

Como excepción, las personas a las que se refiere el párrafo anterior no podrán acceder a los datos del causante, ni solicitar su rectificación o supresión, cuando la persona fallecida lo hubiese prohibido expresamente o así lo establezca una ley. Dicha prohibición no afectará al derecho de los herederos a acceder a los datos de carácter patrimonial del causante.

2. Las personas o instituciones a las que el fallecido hubiese designado expresamente para ello podrán también solicitar, con arreglo a las instrucciones recibidas, el acceso a los datos personales de este y, en su caso su rectificación o supresión.

Mediante real decreto se establecerán los requisitos y condiciones para acreditar la validez y vigencia de estos mandatos e instrucciones y, en su caso, el registro de los mismos.

3. En caso de fallecimiento de menores, estas facultades podrán ejercerse también por sus representantes legales o, en el marco de sus competencias, por el Ministerio Fiscal, que podrá actuar de oficio o a instancia de cualquier persona física o jurídica interesada.

En caso de fallecimiento de personas con discapacidad, estas facultades también podrán ejercerse, además de por quienes señala el párrafo anterior, por quienes hubiesen sido designados para el ejercicio de funciones de apoyo, si tales facultades se entendieran comprendidas en las medidas de apoyo prestadas por el designado.»

«Artículo 96. Derecho al testamento digital.

1. El acceso a contenidos gestionados por prestadores de servicios de la sociedad de la información sobre personas fallecidas se regirá por las siguientes reglas:

a) Las personas vinculadas al fallecido por razones familiares o de hecho, así como sus herederos podrán dirigirse a los prestadores de servicios de la sociedad de la información al objeto de acceder a dichos contenidos e impartirles las instrucciones que estimen oportunas sobre su utilización, destino o supresión.

Como excepción, las personas mencionadas no podrán acceder a los contenidos del causante, ni solicitar su modificación o eliminación, cuando la persona fallecida lo hubiese prohibido expresamente o así lo establezca una ley. Dicha prohibición no afectará al derecho de los herederos a acceder a los contenidos que pudiesen formar parte del caudal relicto.

b) El albacea testamentario así como aquella persona o institución a la que el fallecido hubiese designado expresamente para ello también podrá solicitar, con arreglo a las instrucciones recibidas, el acceso a los contenidos con vistas a dar cumplimiento a tales instrucciones.

c) En caso de personas fallecidas menores de edad, estas facultades podrán ejercerse también por sus representantes legales o, en el marco de sus competencias, por el Ministerio Fiscal, que podrá actuar de oficio o a instancia de cualquier persona física o jurídica interesada.

d) En caso de fallecimiento de personas con discapacidad, estas facultades podrán ejercerse también, además de por quienes señala la letra anterior, por quienes hubiesen sido designados para el ejercicio de funciones de apoyo si tales facultades se entendieran comprendidas en las medidas de apoyo prestadas por el designado.

2. Las personas legitimadas en el apartado anterior podrán decidir acerca del mantenimiento o eliminación de los perfiles personales de personas fallecidas en redes sociales o servicios equivalentes, a menos que el fallecido hu-

biera decidido acerca de esta circunstancia, en cuyo caso se estará a sus instrucciones.

El responsable del servicio al que se le comunique, con arreglo al párrafo anterior, la solicitud de eliminación del perfil, deberá proceder sin dilación a la misma.

3. Mediante real decreto se establecerán los requisitos y condiciones para acreditar la validez y vigencia de los mandatos e instrucciones y, en su caso, el registro de los mismos, que podrá coincidir con el previsto en el artículo 3 de esta ley orgánica.

4. Lo establecido en este artículo en relación con las personas fallecidas en las comunidades autónomas con derecho civil, foral o especial, propio se regirá por lo establecido por estas dentro de su ámbito de aplicación.»

En otro sentido, la DDP no hace mención expresa a las personas fallecidas, si bien, el legislador español, en la LOPDP adopta determinadas previsiones específicas para clarificar el procedimiento a seguir en algunos supuestos.

El artículo 3 prescribe que las personas vinculadas al fallecido por razones familiares o, de hecho, así como sus herederos, podrán dirigirse al responsable o encargado del tratamiento al objeto de solicitar el acceso, rectificación o supresión de los datos de aquel, de acuerdo con lo dispuesto en la ley orgánica.

En el caso de fallecimiento de menores, estas facultades podrán ejercerse también por sus representantes legales o, en el marco de sus competencias, por el Ministerio Fiscal, que podrá actuar de oficio o a instancia de cualquier persona interesada y en el caso de personas fallecidas que hubiesen tenido alguna discapacidad, estas facultades también podrán ejercerse, además de por quienes señala el apartado anterior, por quienes hubiesen sido designados para el ejercicio de funciones de apoyo, si tales facultades se entendieran comprendidas en las medidas de apoyo prestadas por el designado.

En el caso específico de las personas con discapacidad la Ley Orgánica obliga al responsable a deberá facilitar al interesado en todos los supuestos en los que debe relacionarse con esta persona que esto se efectué de forma concisa, inteligible, de fácil acceso y con lenguaje claro y sencillo para todas las personas, incluidas aquellas con discapacidad.

Como conclusión, se podría argumentar que los datos de estas personas que figuren en los tratamientos con finalidades policiales estarán sujetos a las previsiones de los responsables y a la legislación vigente a la hora de facilitar o no su posterior uso o tratamiento.

A modo de ejemplos, podemos ver el sistema establecido por la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.

En sus artículos 17 a 19 se dispone el sistema de conservación, acceso y custodia de las historias clínicas de los pacientes.

El artículo 18.4 indica:

«4. Los centros sanitarios y los facultativos de ejercicio individual sólo facilitarán el acceso a la historia clínica de los pacientes fallecidos a las personas vinculadas a él, por razones familiares o de hecho, salvo que el fallecido lo hubiese prohibido expresamente y así se acredite. En cualquier caso, el ac-

ceso de un tercero a la historia clínica motivado por un riesgo para su salud se limitará a los datos pertinentes. No se facilitará información que afecte a la intimidad del fallecido ni a las anotaciones subjetivas de los profesionales, ni que perjudique a terceros.»

Y el artículo 17, en sus apartados 1 y 2, dispone los plazos mínimos de conservación de la siguiente forma:

«Artículo 17. La conservación de la documentación clínica.

1. Los centros sanitarios tienen la obligación de conservar la documentación clínica en condiciones que garanticen su correcto mantenimiento y seguridad, aunque no necesariamente en el soporte original, para la debida asistencia al paciente durante el tiempo adecuado a cada caso y, como mínimo, cinco años contados desde la fecha del alta de cada proceso asistencial.

No obstante, los datos de la historia clínica relacionados con el nacimiento del paciente, incluidos los resultados de las pruebas biométricas, médicas o analíticas que en su caso resulten necesarias para determinar el vínculo de filiación con la madre, no se destruirán, trasladándose una vez conocido el fallecimiento del paciente, a los archivos definitivos de la Administración correspondiente, donde se conservarán con las debidas medidas de seguridad a los efectos de la legislación de protección de datos.

2. La documentación clínica también se conservará a efectos judiciales de conformidad con la legislación vigente. Se conservará, asimismo, cuando existan razones epidemiológicas, de investigación o de organización y funcionamiento del Sistema Nacional de Salud. Su tratamiento se hará de forma que se evite en lo posible la identificación de las personas afectadas.

Sin perjuicio del derecho al que se refiere el artículo siguiente, los datos de la historia clínica relacionados con las pruebas biométricas, médicas o analíticas que resulten necesarias para determinar el vínculo de filiación con la madre del recién nacido, sólo podrán ser comunicados a petición judicial, dentro del correspondiente proceso penal o en caso de reclamación o impugnación judicial de la filiación materna....(...)...»

A resultas de la problemática surgida de los distintos usos de los datos de personas fallecidas es interesante valorar que esta cuestión sería posible si el interesado no se ha opuesto de manera que se deje constancia en el tráfico jurídico o si las disposiciones legales no lo prohíben para el supuesto específico a llevar a cabo[100].

[100] https://elpais.com/economia/2021-08-13/el-derecho-de-resucitar-digitalmente-a-los-muertos.html

VI. POLÍTICA DE SEGURIDAD DEL MINISTERIO DEL INTERIOR

1. Descripción de la Orden Ministerial

La Orden INT/424/2019, de 10 de abril, por la que se aprueba la política de seguridad de la información en el ámbito de la administración electrónica del Ministerio del Interior y las directrices generales en materia de seguridad de la información para la difusión de resultados provisionales en procesos electorales.

Se compone de 30 artículos divididos en dos capítulos, el primero describe la Política de Seguridad de la Información del Ministerio del Interior en el ámbito de la administración electrónica y el segundo dispone las directrices de seguridad de la información para la difusión de resultados provisionales en materia de procesos electorales. Finalizando con una disposición adicional, una derogatoria y dos disposiciones finales.

Esta PSI identifica las distintas responsabilidades y establece los principios y directrices para una protección apropiada y consistente de los servicios y activos de información gestionados en el ámbito de competencias del Ministerio del Interior, estableciendo el marco organizativo y tecnológico de la misma. El Ministro dispone que se apliquen los principios básicos y requisitos mínimos del Esquema Nacional de Seguridad[101] de forma que se logre una protección adecuada de la información y los servicios del Departamento, fijando los ámbitos objetivo y subjetivo de aplicación al trasladar, por un lado, que será de aplicación a los sistemas de información y activos utilizados por el Ministerio del Interior en la prestación de los servicios de administración electrónica y, por otro lado, imponer su obligado cumplimiento por todo el personal con acceso a los sistemas de información con independencia de cuál sea su destino, adscripción o relación con el Ministerio así como para todos los órganos y unidades de este Órgano superior, así como para los organismos públicos dependientes del mismo[102].

2. Estructura orgánica de protección de datos

Según la LOPDP las funciones la posición de los Delegados de Protección de Datos y sus misiones serán las recogidas en el artículo 42:

> *«Artículo 42. Funciones del delegado de protección de datos.*
>
> *El responsable del tratamiento encomendará al delegado de protección de datos, al menos, las siguientes funciones:*
>
> *a) Informar y asesorar al responsable del tratamiento y a los empleados que se ocupen del mismo, acerca de las obligaciones que les incumben en*

[101] Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

[102] FERNÁNDEZ GONZÁLEZ. C.M. AYLLÓN SANTIAGO, H.S. Prólogo: Jorge Álvaro Navas Elorza *«Tratamiento de datos de carácter personal en el ámbito policial» ISBN:978-84-290-2433-3 Editorial Reus. 1ª Edición.*

virtud de esta ley orgánica y de otras disposiciones de protección de datos aplicables.

b) Supervisar el cumplimiento de lo dispuesto en esta ley orgánica y en otras disposiciones de protección de datos aplicables, así como de lo establecido en las políticas del responsable del tratamiento en materia de protección de datos personales, incluidas la asignación de responsabilidades, la concienciación y formación del personal que participe en las operaciones de tratamiento y las auditorías correspondientes.

c) Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su realización.

d) Cooperar con la autoridad de protección de datos en los términos de la legislación vigente.

e) Actuar como punto de contacto de la autoridad de protección de datos para las cuestiones relacionadas con el tratamiento, incluida la consulta previa referida en el artículo 36, y realizar consultas, en su caso, sobre cualquier otro asunto.»

La Orden ministerial que establece la PSI, crea también un órgano colegiado denominado el Grupo de Trabajo de los Delegados de Protección de Datos (GTDPD), que está compuesto por los DPD nombrados en el Ministerio:

- DPD del Ministerio, para el ámbito del Ministro, y de la Subsecretaría del Interior (excluida la Dirección General de Tráfico).
- DPD de la Secretaría de Estado de Seguridad.
- DPD de la Secretaría General de Instituciones Penitenciarias
- DPD de la Dirección General de la Policía.
- DPD de la Dirección General de la Guardia Civil.
- DPD de la Secretaría General de Instituciones Penitenciarias.
- DPD de la Dirección General de Tráfico.

En este grupo, asistiría el Responsable de Protección de Datos PNR de la ONIP, ya que, en lo no dispuesto en la LOPNR, se le aplica las normas referidas a los DPD en la DDP.

Como puede observarse, el citado instrumento reglamentario no diferencia sobre si la actuación de los DPD está bajo el paraguas del RGPD u otra normativa, si bien, en la parte expositiva si recoge que se aplicarán asimismo los presupuestos de la DDP (incluso tras la promulgación de la LOPNR, deberá hacerse cargo de los tratamientos PNR), por lo que el GTDPD y sus miembros ejercerán sus funciones en el ámbito competencial de estas normas.

Esto ha quedado meridianamente claro con la promulgación de la LOPDP que en su artículo 40.2 dispone que:

«En el caso de estar designado un delegado de protección de datos al amparo del Reglamento General de Protección de Datos, este será el que asumirá las funciones de delegado de protección de datos previstas en esta ley orgánica.»

El GTDPD ejercerá sus funciones, que podrán ser ampliadas dentro su ámbito competencial, lo cual resulta obvio, según lo apuntado previamente:

- Supervisar la normativa de seguridad del ministerio en relación al cumplimiento de lo dispuesto en el Reglamento general de protección de datos, en otras disposiciones de protección de datos de la Unión Europea o de los Estados miembros en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes.
- Normalizar metodologías de acción, criterios comunes y documentación general a utilizar en materia de protección de datos personales.
- Proponer recomendaciones o sugerencias que considere oportunas relativas a materia de protección de datos a los responsables y encargados de tratamiento del Ministerio del Interior.
- En las reuniones del GTDPDS podrán participar cuantos asesores, internos o externos, estimen necesarios los miembros del mismo.

La meta de garantizar el derecho a la protección de datos de carácter personal en las actividades de tratamiento del Departamento, es un objetivo compartido por todas las unidades que lo componen y se regirá por los principios del tratamiento recogidos en las normas de la Unión Europea (RGPD y Directivas) y en los Acuerdos y Tratados Internacionales firmados por España.

Para lograr dichas finalidades, se procedió a nombrar los DPD que forman el GTDPD y a designar al Responsable de Protección de datos PNR. Las actuaciones de los mismos se rigen por el principio de independencia, por lo que no recibirán ninguna instrucción en lo que respecta al desempeño de sus funciones y podrán estar asistidos por grupos de trabajo integrados por representantes de las unidades administrativas de su ámbito de actuación.

Sin perjuicio de todas las funciones y obligaciones que tienen derivadas del RGPD, (en especial los artículos 37 a 39), en la DDP (en especial artículos 32 a 34) y en la LOPNR (artículos 8 y 15), se les encomienda las siguientes tareas específicas:

- Asesorar a los titulares de los Centros Directivos para determinar los responsables de tratamiento en los casos en los casos en que no se corresponda la definición legal de responsable con el titular de la unidad en que se produzca la operación o haya varias unidades en las que se produzca la operación.
- Dar instrucciones sobre la RAT y facilitar el apoyo necesario para el mantenimiento del citado registro.
- Actuar como intermediario con los ciudadanos y otras administraciones en los casos en los que los responsables de tratamiento deban atender las mismas.
- Recibir las peticiones que se dirijan a ellos a los responsables de tratamiento.

- Proporcionar asesoramiento y herramientas específicas tanto para esta gestión de riesgos, como para la realización de evaluaciones de impacto en la privacidad para los tratamientos, en especial los de alto riesgo, previa petición del responsable del tratamiento.
- Facilitar modelos de cláusulas tipo y asesoramiento para la adecuación de contratos, acuerdos y convenios que incluyan el tratamiento de datos personales.
- Definir los protocolos correspondientes, coordinados con los responsables de seguridad, para la comunicación de brechas de seguridad que afecten a información con datos de carácter personal.
- Concretar y difundir un procedimiento de privacidad desde el diseño que tendrá por objetivo el introducir un protocolo dentro del ciclo de vida del desarrollo y mantenimiento de sistemas de información que garantice que se tienen en cuenta las exigencias de seguridad derivadas del manejo de datos personales.
- Fomentar procesos de auditoría periódica encaminados a la mejora continua del cumplimiento normativo en materia de protección de datos y a la implantación de las medidas correctoras necesarias para mejorar la seguridad de los datos personales.
- Planificar actuaciones periódicas de formación y concienciación al personal en materia de privacidad e impulsar la formación en materia de gestión documental y archivo.

Es importante resaltar que la PSI establece la previsión mediante la cual se recoge, en relación con los sistemas de información que manejen datos de carácter personal, que prevalecerán las mayores exigencias contenidas en la normativa de protección de datos en vigor que afecte al sistema de información concreto[103].

[103] FERNÁNDEZ GONZÁLEZ. C.M. AYLLÓN SANTIAGO, H.S. Prólogo: Jorge Álvaro Navas Elorza *«Tratamiento de datos de carácter personal en el ámbito policial» ISBN:978-84-290-2433-3 Editorial Reus. 1ª Edición.*

CAPÍTULO 2
PANORAMA LEGISLATIVO

I. ANÁLISIS DE LA NORMATIVA DE PROTECCIÓN DE DATOS DE LA UNIÓN EUROPEA CON INCIDENCIA EN LA ACTIVIDAD POLICIAL

1. Antecedentes

Aunque el rápido desarrollo de las tecnologías de la información y la comunicación durante el presente siglo han puesto de actualidad la acuciante necesidad de articular un sistema de protección de la intimidad de las personas frente a la exposición de sus datos en el ámbito digital, el marco jurídico de la protección de datos de carácter personal no es en absoluto una creación reciente, sino que, partiendo de unos planteamientos embrionarios, ha sido el resultado de un largo y gradual proceso de decantación y consolidación que se ha prolongado a lo largo de varias décadas.

En su redacción original, el artículo 286 del Tratado Constitutivo de la Comunidad Europea, de 26 de marzo de 1957, proclamaba de forma muy genérica que toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.

A su vez, el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, conocido generalmente como la Convención Europea de Derechos Humanos, suscrito en Roma el 4 de noviembre de 1950, y enmendado posteriormente por medio de Protocolos adicionales, reconocía en su artículo 8, también en términos genéricos el derecho de toda persona al respeto de su vida privada y familiar.

Posteriormente, el Convenio 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, cuyo texto ha sido actualizado en 2018, constituyó el primer instrumento internacional jurídicamente vinculante adoptado en el ámbito de la protección de datos. Conforme a su artículo 1, tiene como fin garantizar a cualquier persona física el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona.

El Convenio es de aplicación a los ficheros y a los tratamientos automatizados de datos de carácter personal en los sectores público y privado, siendo destacable el esfuerzo por concretar el contenido de los principales conceptos básicos que se refieren a la materia de protección de datos, definiendo a continuación los datos de carácter personal como cualquier información relativa a una persona física identificada o identificable; los ficheros automatizados como cualquier conjunto de informaciones que sea objeto de tratamiento automatizado; y entendiendo por tratamiento automatizado las operaciones que a continuación se indican, efectuadas en su totalidad o en parte con ayuda de procedimientos automatizados: Registro de datos, aplicación a esos datos de operaciones lógicas aritméticas, su modificación, borrado, extracción o difusión.

De acuerdo con este Convenio, los datos de carácter personal que revelen el origen racial, las opiniones políticas, las convicciones religiosas u otras convicciones, así como los datos de carácter personal relativos a la salud o a la vida sexual, no podrán tratarse automáticamente a menos que el derecho interno prevea garantías apropiadas. La misma norma regirá en el caso de datos de carácter personal referentes a condenas penales. Asimismo, exige a los países firmantes la adopción de medidas de seguridad apropiadas para la protección de los datos de carácter personal registrados en ficheros automatizados contra la destrucción accidental o no autorizada, o la pérdida accidental, así como contra el acceso, la modificación o la difusión no autorizados.

En este contexto, en el ámbito comunitario cobra importancia la Recomendación de la Comisión Europea, de 29 de julio de 1981, relativa al Convenio del Consejo de Europa sobre protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, en la que se sientan las bases de lo que sería la primera aproximación de la Unión Europea al establecimiento de un marco jurídico uniforme y exhaustivo en la materia.

La Recomendación considera que con la generalización del tratamiento electrónico de datos y su creciente uso, la protección de datos se convierte en un elemento necesario de la protección del individuo y constituye uno de sus derechos fundamentales, valorando como deseable que se lleve a cabo en todos los Estados miembros de la Comunidad una aproximación en materia de protección de datos que supere las divergencias existentes entre las distintas legislaciones nacionales, recomendando a los Estados miembros la firma del citado Convenio del Consejo de Europa, y reservándose el derecho a promover una norma específica al respecto.

La norma específica adoptada finalmente por la Unión Europea fue 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, que fue norma básica en la materia y mantuvo su vigencia hasta que fue sustituida en 2016 por el Reglamento General de Protección de Datos.

Esta Directiva toma como punto de partida de su regulación el mercado interior de la Unión Europea y la libre circulación de mercancías, personas, servicios y capitales, en la medida en que la misma también implica la libre circulación de datos de carácter personal de un Estado a otro, entendiendo que las diferencias jurídicas en la regulación de cada Estado en esta materia obstaculizan ese flujo

transfronterizo. Por ello, las instituciones comunitarias consideraron imperativo si no homogeneizar, al menos armonizar las legislaciones nacionales en materia de protección de datos de carácter personal, entendiéndolo como una herramienta para impedir las trabas a la libre circulación de información personal en el contexto del mercado interior, y evitar que la defensa de los derechos fundamentales se torne en freno para los objetivos de la integración económica.

Por tanto, a diferencia del Convenio 108 del Consejo de Europa, la Directiva no es un instrumento directamente orientado a la protección de los derechos de las personas, aunque indirectamente alcance dicho objetivo, y tiene un ámbito de aplicación sustancialmente más restringido que aquel.

Esta dualidad se explicita en la redacción de su artículo 1, relativa al objetivo de la Directiva:

> *«1. Los Estados miembros garantizarán, con arreglo a las disposiciones de la presente Directiva, la protección de las libertades y de los derechos fundamentales de las personas físicas, y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales.*
>
> *2. Los Estados miembros no podrán restringir ni prohibir la libre circulación de datos personales entre los Estados miembros por motivos relacionados con la protección garantizada en virtud del apartado 1.»*

Asimismo, conforme a su artículo 3, la Directiva se aplica al tratamiento total o parcialmente automatizado de datos personales e, igualmente, al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero, con lo que el soporte en que se consignan los datos personales no es particularmente relevante, y además, quedan excluidos de su regulación los tratamiento realizados en ejercicio de actividades no comprendidas en el ámbito de aplicación del Derecho comunitario, citando expresamente entre estas excepciones a su regulación el «tratamiento de datos que tenga por objeto la seguridad pública, la defensa, la seguridad del Estado» y las actividades del Estado en materia penal.

Con tales salvedades y limitaciones, la Directiva contenía normas de autorregulación de los diferentes sectores que utilizaban tratamientos de datos personales, y recogía de forma considerablemente detallada los principios que, como mínimo, debían acoger las normas nacionales en materia de protección de datos personales, así como los criterios a tomar en consideración para el intercambio de datos personales entre los distintos Estados miembros, en línea con la finalidad de preservar el mercado interior que constituía el objetivo fundamental de la Directiva. En el mismo sentido, también se regulaba la cesión de datos a terceros países, erigiendo a la Comisión Europea en el principal garante del cumplimiento por parte del tercer Estado de medidas de seguridad suficientes, aunque introduciendo, al mismo tiempo, un amplio régimen de excepciones por los que los estados miembros podían justificar la cesión aun cuando no se garantizaran tales niveles de seguridad.

Por último, dado que la protección de datos personales se consideraba un aspecto básico de la tutela de los derechos de los ciudadanos, la Directiva exigió a los Estados miembros la habilitación de una o más autoridades públicas que se encargasen de velar por la aplicación en su territorio de la normativa adoptada en

aplicación de la Directiva, aunque sin concretar el modelo institucional de dichas autoridades, más allá de exigirles independencia en el ejercicio de sus funciones, entendida como no sujeción a instrucciones.

2. Las bases del régimen de protección de datos de carácter personal

Trascurrido poco tiempo tras la aprobación de la Directiva 95/46/CE, la propia Unión Europea dio inicio a una profunda revisión del régimen de la protección de datos de carácter personal bajo una perspectiva más amplia y orientada a la protección de los derechos de las personas, dentro de una visión general que pretendía rediseñar las bases de la Unión Europea mediante la reforma de sus actos fundacionales, buscando una mayor integración política situando, al mismo tiempo, a la persona en el centro de la actuación de la Unión Europea.

El 18 de junio de 2003, se aprobó el proyecto del Tratado por el que se establecía una Constitución para Europa, conocido simplemente como Constitución Europea, destinado a crear un texto constitucional consolidado para la Unión Europea que, de haber sido aprobado, habría reemplazado los tratados fundacionales existentes con un solo texto, otorgado fuerza legal a la Carta de los Derechos Fundamentales de la Unión Europea, y sustituyendo por un sistema de mayoría cualificada el procedimiento de votación en diversas áreas de política que previamente se habían decidido por unanimidad, facilitando así el proceso de toma de decisiones y dando primacía a las instituciones Europeas frente a los estados miembros, reforzando los símbolos y las instituciones comunes sobre los nacionales con vistas a una futura y gradual integración política.

Sin embargo, aunque fue firmado en Roma por los jefes de gobierno de los países que formaban la Unión y, el 12 de enero de 2005, el Parlamento Europeo aprobó una resolución por amplia mayoría en la que recomendaba a los Estados miembros que ratificaran la nueva Constitución, el resultado de los referéndums a los que fue sometido en Francia y Países Bajos fue negativo, presagiándose el mismo resultado en otros países, por lo que se suspendió su celebración.

Estas circunstancias provocaron en la Unión Europea una profunda sensación de fracaso y crisis, con menoscabo de los soportes políticos y sociales que la sostenían, así como una parálisis institucional que únicamente comenzó a superarse durante la presidencia alemana de la Unión, a partir de 2007. Bajo el impulso alemán se abandonaron los elementos más identificados con el llamado proceso constitucional, y los esfuerzos se centraron en recuperar buena parte de los avances que ya se habían debatido y acordado, por la vía europea tradicional de la reforma de los Tratados, lo que finalmente alumbró un Tratado de Reforma firmado por los Jefes de Estado y Gobierno el 13 de diciembre de 2007 en Lisboa.

El nuevo régimen jurídico para la protección de datos de carácter personal definido por los acontecimientos políticos descritos se encuentra construido sobre las siguientes normas:

- La Carta de los Derechos Fundamentales de la Unión Europea:

El actual marco jurídico de la protección de datos de carácter personal en el ámbito de la Unión Europea nace precisamente con la Carta de los Derechos Fundamentales de la Unión Europea. Este texto busca, por primera vez, reunir en un

único documento todos los derechos que hasta ese momento se encontraban diseminados en distintos instrumentos legislativos nacionales e internacionales, y fue proclamado por el Parlamento Europeo, la Comisión Europea y el Consejo de la Unión Europea el 7 de diciembre del año 2000, y del que se adoptó una versión revisada el 12 de diciembre de 2007 en Estrasburgo.

Su artículo 8 se consagra expresamente a la protección de datos de carácter personal, con el siguiente texto:

> *«1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.*
>
> *2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación.*
>
> *3. El respeto de estas normas quedará sujeto al control de una autoridad independiente.»*

- El Tratado de Funcionamiento de la Unión Europea:

Este texto, junto con el Tratado de la Unión Europea, constituyen actualmente los dos Tratados sobre los que se fundamenta la Unión. La redacción actual de uno y otro fue introducida por medio del Tratado de Lisboa, firmado el 13 de diciembre de 2007, y cuya entrada en vigor tuvo lugar el 1 de diciembre de 2009. El artículo 16 del Tratado de Funcionamiento de la Unión Europea incorpora y actualiza el texto del antiguo artículo 286 del Tratado Constitutivo de la Comunidad Europea, de 26 de marzo de 1957, en los términos siguientes:

> *«1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.*
>
> *2. El Parlamento Europeo y el Consejo establecerán, con arreglo al procedimiento legislativo ordinario, las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por las instituciones, órganos y organismos de la Unión, así como por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión, y sobre la libre circulación de estos datos. El respeto de dichas normas estará sometido al control de autoridades independientes. Las normas que se adopten en virtud del presente artículo se entenderán sin perjuicio de las normas específicas previstas en el artículo 39 del Tratado de la Unión Europea.»*

- El Tratado de la Unión Europea:

A su vez, el texto consolidado del Tratado de la Unión Europea, modificado igualmente a través del Tratado de Lisboa, y como complemento de la regulación introducida en el Tratado de Funcionamiento de la Unión Europea, señala en su artículo 39:

> *«De conformidad con el artículo 16 del Tratado de Funcionamiento de la Unión Europea, y no obstante lo dispuesto en su apartado 2, el Consejo adoptará una decisión que fije las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por los Estados miem-*

bros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del presente capítulo, y sobre la libre circulación de dichos datos. El respeto de dichas normas estará sometido al control de autoridades independientes.»

3. Principales instrumentos normativos de la Unión Europea en materia de protección de datos

Llegados a este punto, y tomando como elemento de partida el tratamiento de la protección de datos de carácter personal recogido en la actual redacción de los Tratados constitutivos de la Unión Europea, ésta dio inicio a un ambicioso proceso destinado a afrontar las implicaciones de la actual revolución digital mediante la definición de un régimen jurídico cada vez más uniforme sobre la protección de datos personales que proporcionara un marco legal de referencia para la implementación de una verdadera cultura de garantía de la privacidad y protección de los datos personales en la Unión Europea en un entorno social cada vez más globalizado. Empero, este proceso, aunque ha actualizado y armonizado la regulación sobre la materia tanto nacional como europea, no ha puesto fin a la dispersión normativa existente.

En consecuencia, y sin ánimo de exhaustividad, los principales instrumentos normativos de la Unión Europea actualmente vigentes en materia de protección de datos con un impacto más significativo en los tratamientos de datos realizados con fines o por instituciones policiales, son los siguientes:

- El Reglamento General de Protección de Datos:

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 por el que se deroga la Directiva 95/46/CE, cuya entrada en vigor tuvo lugar en mayo de 2018. El Reglamento general de protección de datos es una norma que pretende tener alcance general, y busca, con su eficacia directa, superar los obstáculos que impidieron la finalidad armonizadora que en su momento persiguió la derogada Directiva 95/46/CE, que a través de los procesos nacionales de transposición acabó desembocando en un mosaico normativo con perfiles irregulares en los distintos Estados miembros, con apreciables diferencias en cuanto a la protección de los derechos en unos y otros.

Su objetivo es proteger a todos los ciudadanos de la Unión Europea frente a las violaciones de la privacidad y de sus datos personales, creando, al mismo tiempo, un marco de actuación más claro y coherente para la actuación de las empresas. A tal fin, el Reglamento general de protección de datos atiende a nuevas circunstancias, principalmente el aumento de los flujos transfronterizos de datos personales como consecuencia del funcionamiento del mercado interior, y a los retos planteados por la rápida evolución tecnológica y la globalización, que han convertido la información de carácter personal en un recurso fundamental de la sociedad de la información, reforzando la seguridad jurídica y transparencia.

Entre los derechos más significativos que se reconocen a los ciudadanos se encuentra la exigencia de un consentimiento claro y expreso para el tratamiento de sus datos y el derecho a recibir información clara y comprensible sobre el

mismo; el derecho al olvido, en base al cual un ciudadano puede solicitar que se supriman sus datos; la libertad de transferir sus datos de un proveedor de servicios a otro; así como el derecho a saber si sus datos han sido pirateados. Estas nuevas normas son de aplicación a todas empresas que operan en la Unión Europea, aunque tengan su sede fuera de ella. Asimismo, será posible imponer medidas correctoras, tales como advertencias y órdenes, o sanciones a las empresas que las infrinjan.

- La Directiva sobre protección de datos en el ámbito penal y policial:

En la misma fecha que el Reglamento General de Protección de Datos también entró en vigor la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y la libre circulación de dichos datos, y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.

Esta norma garantiza el derecho fundamental de los ciudadanos a la protección de sus datos cuando los mismos son utilizados por las autoridades encargadas de hacer cumplir la ley en el ejercicio de sus funciones. A través de la misma se garantiza que los datos personales de las víctimas, testigos y sospechosos de delitos sean debidamente protegidos y facilita la cooperación transfronteriza entre las autoridades competentes en la lucha contra la delincuencia y el terrorismo. Esta norma está llamada a ser la piedra angular de los tratamientos de datos realizados por las instituciones competentes en materia de seguridad pública, pero no la única, ya que cuando dichas autoridades traten datos personales con fines distintos de los previstos en la presente Directiva, se aplica el Reglamento (UE) 2016/679.

- La Directiva relativa a la utilización de datos del registro de nombres de los pasajeros (PNR):

La Directiva (UE) 2016/681 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la utilización de datos del registro de nombres de los pasajeros (PNR) para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave, busca garantizar la protección de la vida y la seguridad de los ciudadanos habilitando a tal fin un marco jurídico para la protección de los datos de los pasajeros utilizados por las autoridades competentes con las finalidades señaladas, para cuya prevención e investigación resulta imprescindible su tratamiento.

Con anterioridad a la aprobación de la presente Directiva ya existía en el ámbito comunitario otra norma que imponía a las compañías aéreas la obligación de comunicar los datos de los pasajeros transportados por ellas, aunque con una finalidad diferente. Se trata de los datos API (*Advance Passsenger Information*), cuyo propósito era mejorar los controles fronterizos y combatir la inmigración ilegal, por lo que la Directiva (UE) 2016/681 resulta más amplia en cuanto a su finalidad o justificación para recabar los datos citados.

La Directiva (UE) 2016/681 no impone una obligación adicional a las compañías aéreas que ya trataban los datos API y PNR para sus fines comerciales propios, habilitando simplemente la posibilidad de facilitar dichos datos a las autoridades correspondientes con objeto de responder a la amenaza de delitos de terrorismo y de la delincuencia grave, descubrir a los delincuentes y las organizaciones a las que pertenecen, y recabar las pruebas correspondientes para su enjuiciamiento con garantías.

- La Directiva sobre uso de datos financieros en el ámbito penal y policial:

Se trata de la Directiva (UE) 2019/1153 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, por la que se establecen normas destinadas a facilitar el uso de información financiera y de otro tipo para la prevención, detección, investigación o enjuiciamiento de infracciones penales y por la que se deroga la Decisión 2000/642/JAI del Consejo.

Esta norma persigue un propósito similar al de la Directiva (UE) 2016/681, como es el uso de cierto tipo de información para logar la prevención, detección, investigación o enjuiciamiento de delitos, si bien en este caso mediante la habilitación para el acceso y tratamiento de datos e información de carácter financiero. De igual modo que en la Directiva (UE) 2016/681, también se prevé que los datos sean transmitidos a una Unidad única de información, aunque en este caso de carácter financiero (UIF), y con la finalidad específica de luchar contra delitos de esta naturaleza, como el blanqueo de capitales, financiación de terrorismo, delitos fiscales, etc.

Con objeto de lograr dichas finalidades se articula la creación en los Estados miembros de registros centralizados de cuentas bancarias y de pagos o cajas de seguridad, que serán accesibles por las citadas Unidades (UIF), sin perjuicio de que también puedan serlo para las autoridades y organismos que el Estado haya facultado expresamente para ello.

Aunque tal y como prevé el artículo 25 de la citada norma el plazo de transposición a los ordenamientos nacionales finalizó el 1 de agosto de 2021, España todavía no ha promulgado la correspondiente Ley, si bien se encuentra actualmente en avanzado estado de tramitación.

- La Directiva sobre la privacidad de las comunicaciones electrónicas:

La Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, modificada mediante la Directiva 2009/136/CE, de 25 de noviembre de 2009, trata de establecer nuevas medidas de garantía en materia de protección de datos de carácter personal en relación con el uso de las nuevas tecnologías digitales avanzadas y su rápida implantación y expansión, actualizando la normativa comunitaria ya existente hasta ese momento.

De este modo, los nuevos servicios de comunicaciones electrónicas introducen nuevas posibilidades para los usuarios, pero también traen crecientes riesgos y amenazas que tratan de atajarse por medio de esta Directiva, con objeto de que las diferentes legislaciones de los Estados miembros se armonicen y así poder evitar obstáculos para el mercado interior de las comunicaciones electrónicas.

Como ya se ha apuntado, esta norma fue modificada por la Directiva 2009/136/CE, de 25 de noviembre de 2009, en aras de conseguir un espacio único de información y de una sociedad de la información. Con arreglo a ello, se pretende que los usuarios finales tengan la capacidad de decidir los contenidos que desean enviar y recibir, así como de optar por los servicios, aplicaciones y soportes físicos o lógicos que deseen utilizar para tal fin, sin perjuicio de la necesidad de mantener la integridad y seguridad de las redes y servicios digitales. Para ello las respectivas autoridades nacionales de reglamentación deben promover la capacidad de los usuarios de acceder a la información y distribuirla, y de ejecutar aplicaciones y servicios de su elección. Ante la importancia creciente de las comunicaciones electrónicas tanto para los consumidores como para las empresas, debe facilitarse a los usuarios información completa sobre cualquier limitación concreta que imponga el proveedor del servicio (IP) o de la red en la utilización de los servicios de comunicaciones electrónicas. Dicha información debe especificar, a elección del proveedor, bien sea el tipo de contenido, la aplicación o el servicio de que se trate, bien las aplicaciones o los servicios individuales, bien ambas cosas. En función de la tecnología que se utilice y del tipo de restricción, dichas limitaciones pueden requerir el consentimiento del usuario en virtud de la Directiva 2002/58/CE.

- El Reglamento sobre tratamiento de datos personales por las instituciones y organismos de la Unión:

El 11 de diciembre de 2018 entró en vigor el Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) 45/2001 y la Decisión 1247/2002/CE.

Este Reglamento es de aplicación complementaria al Reglamento General de Protección de Datos, de suerte que ambas normas deben interpretarse de forma homogénea, siendo su finalidad la protección de las personas cuyos datos personales son tratados, ya sea de forma automatizada o no, por las instituciones y organismos de la Unión en cualquier contexto, como puede ser, por ejemplo, porque tengan la condición de empleados de estas instituciones.

Es de señalar que, de igual modo que sucede con el Reglamento General de Protección de Datos, el Reglamento (UE) 2018/1725 no ampara la protección de los datos de las personas jurídicas. Asimismo, es interesante destacar que el Reglamento consagra un capítulo específico, el IX, al tratamiento de datos personales de carácter operativo, tales como los datos personales que, en el marco de investigaciones de infracciones, sean tratados por órganos u organismos de la Unión Europea cuando lleven a cabo actividades en los ámbitos de la cooperación judicial en materia penal y de la cooperación policial, que resultarán de aplicación siempre y cuando no resulten contrarios a lo dispuesto en los capítulos 4 o 5 del Título V del Tratado de Funcionamiento de la Unión Europea y de las normas de la Directiva (UE) 2016/680, que tienen la consideración de normas de carácter especial respecto de este Reglamento.

- La Directiva sobre seguridad de las redes y sistemas de información (Directiva NIS):

La Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión, se desarrolló para dar una respuesta efectiva a los problemas de seguridad de las redes y sistemas de información al entender que era necesario un planteamiento global en la Unión Europea que integrase los requisitos mínimos comunes en materia de desarrollo de capacidades y planificación, intercambio de información, cooperación y requisitos comunes de seguridad para los operadores de servicios esenciales y los proveedores de servicios digitales, sin perjuicio de que esto apliquen medidas de seguridad más estrictas que las previstas en la misma.

El instrumento tiene por objeto lograr un elevado nivel común de seguridad de las redes y sistemas de información dentro de la Unión a fin de mejorar el funcionamiento del mercado interior.

Con este fin se establecen para todos los Estados miembros obligaciones de adoptar una estrategia nacional de seguridad de las redes y sistemas de información; se crea un Grupo de cooperación para apoyar y facilitar la cooperación estratégica y el intercambio entre los Estados miembros y desarrollar la confianza y seguridad ente ellos; también se crea una red de equipos de respuesta a incidentes de seguridad informática (red de CSIRT) con el fin de contribuir al desarrollo de la confianza y seguridad entre los Estados miembros y promover una cooperación operativa rápida y eficaz; se implantan requisitos en materia de seguridad y notificación para los operadores de servicios esenciales y para los proveedores de servicios digitales; y por último, se instauran obligaciones para que los Estados miembros designen autoridades nacionales competentes, puntos de contacto únicos y CSIRT con funciones relacionadas con la seguridad de las redes y sistemas de información.

El Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información cumple con la necesidad de transposición de esta Directiva y, consecuentemente, regula los requisitos y condiciones de seguridad de estas redes y sistemas en el ámbito nacional, implantando, asimismo, un sistema de notificación de incidentes, entendidos como todo suceso inesperado o no deseado cuyas consecuencias redundan en detrimento de la seguridad de aquellas. También establece un marco institucional para la aplicación y para la coordinación entre autoridades competentes y con los órganos de cooperación relevantes en el ámbito comunitario. Su artículo 3 concreta el significado de los principales conceptos que se emplean en materia de ciberseguridad.

La entidad de referencia en España para el desarrollo de la ciberseguridad y de la confianza digital de ciudadanos, empresas y sectores estratégicos es el Instituto Nacional de Ciberseguridad de España (INCIBE), sociedad dependiente del Ministerio de Asuntos Económicos y Transformación Digital a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial. Bajo su gestión, uno de los equipos de respuesta de referencia ante incidentes, que se coordina con el resto de los equipos nacionales e internacionales para mejorar la eficacia en la lucha contra los delitos que involucran a las redes y sistemas de información, reduciendo sus efectos en la seguridad pública es el INCIBE-CERT.

INCIBE-CERT es el centro de respuesta a incidentes de seguridad de referencia para los ciudadanos y entidades de derecho privado en España, que en lo referente a la gestión de incidentes que afecten a operadores críticos del sector privado, y está operado conjuntamente por INCIBE y el Ministerio del Interior, inicialmente a través del Centro Nacional de Protección de Infraestructuras Críticas (CNPIC) y en la actualidad por la Oficina de Coordinación de Ciberseguridad (OCC), ambos dependientes de la Dirección General de Coordinación y Estudios de la Secretaría de Estado de Seguridad.

Por sus implicaciones en los tratamientos de datos derivados de esta materia a nivel nacional no se puede dejar de hacer mención a la Disposición Adicional Novena de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, conforme a la cual:

> *«Cuando, de conformidad con lo dispuesto en la legislación nacional que resulte de aplicación, deban notificarse incidentes de seguridad, las autoridades públicas competentes, equipos de respuesta a emergencias informáticas (CERT), equipos de respuesta a incidentes de seguridad informática (CSIRT), proveedores de redes y servicios de comunicaciones electrónicas y proveedores de tecnologías y servicios de seguridad, podrán tratar los datos personales contenidos en tales notificaciones, exclusivamente durante el tiempo y alcance necesarios para su análisis, detección, protección y respuesta ante incidentes y adoptando las medidas de seguridad adecuadas y proporcionadas al nivel de riesgo determinado.»*

- El Reglamento de Europol:

Europol es una agencia inicialmente creada por medio de la Decisión 2009/371/JAI del Consejo como un ente de la Unión Europea para apoyar y reforzar la actuación de las autoridades competentes de los Estados miembros y su colaboración mutua en la prevención y la lucha contra la delincuencia organizada, el terrorismo y otras formas de delitos graves que afecten a dos o más Estados miembros, y se encuentra actualmente regulada por el Reglamento (UE) 2016/794 del Parlamento Europeo y del Consejo, de 11 de mayo de 2016, relativo a la Agencia de la Unión Europea para la Cooperación Policial (Europol), y por el que se sustituyen y derogan las Decisiones 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI y 2009/968/JAI del Consejo.

En el ejercicio de sus competencias Europol debe elaborar y facilitar análisis estratégicos y evaluaciones de amenazas en la lucha contra la delincuencia, y es un eje para el intercambio de información policial en la Unión Europea, que se alimenta de los datos proporcionados por las instituciones policiales de los distintos Estados miembros. Entre la información recabada, almacenada, procesada, analizada e intercambiada por Europol se incluye la inteligencia criminal referida a la información sobre delitos o actividades delictivas comprendidas en el ámbito de los objetivos de Europol, obtenida con la finalidad de determinar si se ha cometido o puede cometerse en el futuro algún acto delictivo concreto.

Dada la naturaleza de las funciones de Europol, para que pueda cumplir su misión se le permite el tratamiento de todos los datos personales que reciba con el fin de identificar los vínculos entre múltiples áreas e investigaciones de delitos, y no quedar limitada a la detección de conexiones únicamente dentro de un área

delictiva. No obstante, Europol también debe garantizar al mismo tiempo que el tratamiento de todos los datos personales necesarios para análisis operativos reúna los necesarios requisitos de seguridad. Por tal motivo el Reglamento dedica expresamente su Capítulo VI a las garantías de protección de datos.

Con el fin de respetar la propiedad de los datos y la protección de los datos personales, los Estados miembros, los organismos de la Unión, los países terceros y las organizaciones internacionales deben poder determinar la finalidad o finalidades para las cuales Europol puede tratar los datos que facilitan y restringir los derechos de acceso. La limitación de la finalidad es un principio fundamental del tratamiento de datos personales; en particular, contribuye a la transparencia, la seguridad jurídica y la previsibilidad, y reviste especial importancia en el ámbito de la cooperación policial, en el que los interesados no suelen estar al tanto de la recogida y del tratamiento de sus datos personales, y en el que el uso de datos personales puede repercutir de forma muy significativa en las vidas y libertades de las personas físicas.

A fin de garantizar que únicamente tengan acceso a los datos aquellos que lo necesiten para el desempeño de sus tareas específicas, el presente Reglamento debe establecer normas detalladas sobre los diferentes grados del derecho de acceso a los datos tratados por Europol. Tales normas deben entenderse sin perjuicio de las restricciones de acceso impuestas por los proveedores de datos, ya que ha de respetarse el principio de la propiedad de los datos. Con el fin de mejorar la eficiencia en la prevención y la lucha contra los delitos comprendidos en el ámbito de sus objetivos, Europol debe notificar a los Estados miembros la información que les concierna.

Al igual que el resto de las entidades que quedan bajo la normativa europea, por parte de Europol, los datos personales deben ser objeto de un tratamiento equitativo y conforme a la ley, destinados a fines determinados, explícitos y legítimos, sin que puedan ser tratados ulteriormente de forma incompatible con esos fines; deben ser adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados; han de ser exactos y actualizados, adoptando todas las medidas razonables para su cancelación o rectificación cuando proceda; deben ser conservados de forma que permitan la identificación de los interesados y únicamente durante un período no superior al necesario para los fines para los que son tratados; y su tratamiento se hará, en todo caso, de un modo que garantice una seguridad adecuada de los datos personales, especialmente en relación con aquellos que pertenecen a categorías especiales.

- La interoperabilidad de los sistemas de información de la Unión Europea en el ámbito policial

Por último, resulta imprescindible hacer una referencia a dos reglamentos complementarios de indudable trascendencia en cuanto a las posibilidades que abren en materia de interoperabilidad de los sistemas de información policial en el ámbito de la Unión Europea, cuya gestación responde a la iniciativa, impulsada por ésta desde el año 2016, de poner en marcha un proceso, cuya implementación definitiva está prevista a finales de 2023, destinado a lograr la interoperabilidad de los sistemas de información de la UE para la gestión de la seguridad, las fronteras y la migración, con el objetivo de solucionar las deficiencias estructurales

relacionadas con estos sistemas que obstaculizan la labor de las autoridades nacionales y garantizar que los guardias de fronteras, las autoridades aduaneras, los agentes de policía y las autoridades judiciales tengan a su disposición la información necesaria para su actuación.

Estas normas son el Reglamento (UE) 2019/817, del Parlamento Europeo y del Consejo, de 20 de mayo de 2019, relativo al establecimiento de un marco para la interoperabilidad de los sistemas de información de la UE en el ámbito de las fronteras y los visados y por el que se modifican los Reglamentos (CE) 767/2008, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 y (UE) 2018/1861 del Parlamento Europeo y del Consejo, y las Decisiones 2004/512/CE y 2008/633/JAI del Consejo; y el Reglamento (UE) 2019/818, del Parlamento Europeo y del Consejo, de 20 de mayo de 2019, relativo al establecimiento de un marco para la interoperabilidad entre los sistemas de información de la UE en el ámbito de la cooperación policial y judicial, el asilo y la migración y por el que se modifican los Reglamentos (UE) 2018/1726, (UE) 2018/1862 y (UE) 2019/816.

Ambas disposiciones tienen por objeto mejorar la efectividad y la eficiencia de las inspecciones en las fronteras exteriores, contribuir a prevenir y combatir la inmigración ilegal y alcanzar un elevado nivel de seguridad en el espacio de libertad, seguridad y justicia de la Unión (lo que expresamente incluye el mantenimiento de la seguridad pública y del orden público, y la salvaguardia de la seguridad en el territorio de los Estados miembros), mejorar la aplicación de la política común de visados y prestar asistencia en el examen de las solicitudes de protección internacional y en la prevención, detección e investigación de los delitos de terrorismo u otros delitos graves, y ayudar a identificar a las personas desconocidas que no puedan identificarse o los restos humanos sin identificar en caso de catástrofes naturales, accidentes o atentados terroristas. Pese a su condición de Reglamentos, los Estados miembros que deseen acogerse a la posibilidad prevista en estos instrumentos deben adoptar medidas legislativas nacionales al efecto, garantizando el respeto al principio de no discriminación, así como a las garantía y derechos fundamentales de los individuos, especialmente en cuanto a la protección de sus datos personales. En ellas deberán, asimismo, designar a las autoridades competentes para llevar a cabo controles de identidad al amparo de esta normativa, estableciendo los procedimientos, condiciones y criterios para su realización, acordes con el principio de proporcionalidad, previendo, en particular, la facultad del personal de dichas autoridades que ampare la recogida de datos biométricos durante los citados controles de identidad.

Para alcanzar dichos objetivos se pretende implantar la interoperabilidad de los siguientes sistemas de información de la UE: el Sistema de Entradas y Salidas (SES), el Sistema de Información de Visados (VIS), el Sistema Europeo de Información y Autorización de Viajes (SEIAV), Eurodac, el Sistema de Información de Schengen (SIS), y el Sistema Europeo de Información de Antecedentes Penales de nacionales de terceros países (ECRIS-TCN), aunque también se prevé que se incluyan los datos de Europol. Todo ello con el fin de hacer posible que estos sistemas de información y sus datos se complementen mutuamente. Para llevar a efecto las metas propuestas los citados Reglamentos toman como punto de partida que los datos biométricos, como las impresiones dactilares y las imágenes faciales, son únicos y, por tanto, mucho más fiables para la identificación de una persona que

los datos alfanuméricos, contemplándose la creación, como componentes de interoperabilidad, de un portal europeo de búsqueda (PEB), un servicio de correspondencia biométrica compartido (SCB compartido), un registro común de datos de identidad (RCDI) y un detector de identidades múltiples (DIM).

La interoperabilidad de los citados sistemas de información debe permitir a éstos complementarse mutuamente a fin de facilitar la identificación correcta de las personas, facilitando la aplicación técnica y operativa por los Estados miembros de los sistemas de información de la Unión, racionalizando el acceso con fines de prevención, detección o investigación de los delitos de terrorismo u otros delitos graves, y reforzar las garantías de seguridad y protección de los datos que rigen en los respectivos sistemas de información de la UE.

Respecto a los principales componentes del sistema de interoperabilidad, el PEB constituye una herramienta de consulta que, a modo de ventanilla única, tiene por finalidad facilitar técnicamente a las autoridades de los Estados miembros y las agencias de la Unión Europea un acceso rápido, eficiente, sistemático y controlado a los sistemas de información de la UE, así como de los datos de Europol y de las bases de datos de Interpol, en la medida en que resulten necesarios para alcanzar los fines de los sistemas de información de la UE, al permitir la consunta simultanea de todos los sistemas de información relevantes en paralelo. El SBC tendrá por objetivo principal facilitar la identificación de una persona que se encuentre registrada en distintas bases de datos, utilizando un único componente tecnológico para cotejar los datos biométricos de dicha persona entre diferentes sistemas. Estos datos biométricos constituyen datos personales sensibles, por lo que el Reglamento establece salvaguardias para garantizar su tratamiento a los únicos efectos de la identificación inequívoca de las personas afectadas.

Por su parte, el RCDI está destinado a almacenar aquellos datos personales que sean necesarios para permitir una identificación más precisa de las personas cuyos datos están contenidos en aquellos sistemas, incluidos sus datos de identidad, los de su documento de viaje y sus datos biométricos, independientemente del sistema en el que hubiesen sido recogidos originalmente. Solamente deben almacenarse en el RCDI los datos personales estrictamente necesarios para llevar a cabo un control de identidad adecuado, y no deben conservarse durante más tiempo del estrictamente necesario para los fines de los sistemas subyacentes, eliminándose automáticamente cuando los datos se eliminen en éstos. Estos dos Reglamentos especifican que una respuesta de este registro no debe interpretarse como fundamento para extraer conclusiones o tomar medidas con respecto a una persona, sino que solo debe utilizarse para presentar una solicitud de acceso a los sistemas de información subyacentes de la Unión conforme a lo establecido en los mismos y, en su caso, en el Reglamento (UE) 2016/679, de 27 de abril de 2016 (Reglamento General de Protección de Datos); la Directiva (UE) 2016/680, de 27 de abril de 2016, sobre tratamiento de datos personales en el ámbito penal y policial; y el Reglamento (UE) 2018/1725 , de 23 de octubre de 2018, sobre tratamiento de datos personales por las instituciones, órganos y organismos de la Unión.

Por último, la creación del DIM busca respaldar el funcionamiento del RCDI, garantizando la identificación exacta de las personas cuyos datos personales almacenan en los distintos sistemas de información de la UE, para lo que el DIM

debe crear y almacenar vínculos entre los datos obrantes en cada uno de ellos para detectar las identidades múltiples, con la doble finalidad de facilitar los controles de identidad de los viajeros de buena fe y de luchar contra la usurpación de identidad. Solamente contendrá los vínculos los datos de personas que figuran en más de un sistema de información de la UE, y los datos vinculados se limitarán a los imprescindibles para verificar si una persona está registrada, ya sea de forma justificada o injustificada, con diferentes identidades biográficas en diferentes sistemas.

En cuanto a la operativa concreta de la herramienta de interoperabilidad prevista en ambos Reglamentos, se prevé que las consultas del RCDI se lleven a cabo por autoridades policiales, y exclusivamente en los casos siguientes:

> *«a) cuando una autoridad policial no sea capaz de identificar a una persona debido a la falta de un documento de viaje o de otro documento fiable que demuestre su identidad;*
>
> *b) cuando existan dudas sobre los datos de identidad facilitados por una persona;*
>
> *c) cuando existan dudas en cuanto a la autenticidad del documento de viaje u otro documento fiable facilitado por una persona;*
>
> *d) cuando existan dudas en cuanto a la identidad del titular de un documento de viaje o de otro documento fiable; o*
>
> *e) cuando la persona no pueda o se niegue a cooperar.*
>
> *Dicha consulta no estará permitida en el caso de menores de doce años, de no ser en el interés superior del menor.»*

En los supuestos enumerados, las autoridades policiales podrán, únicamente con fines de identificación de una persona, consultar el RCDI con los datos biométricos de la misma tomados en vivo durante un control de identidad, siempre que el procedimiento se haya iniciado en su presencia. Cuando no puedan utilizarse los datos biométricos de la persona o cuando la consulta por estos parámetros sea infructuosa, la consulta se llevará a cabo con los datos de identidad de dicha persona en combinación con los del documento de viaje, o con los datos de identidad facilitados por la misma. Asimismo, se prevé la posibilidad de consulta con los datos biométricos en caso de catástrofe natural, accidente o ataque terrorista, y únicamente con el fin de identificar a personas desconocidas que no puedan identificarse o restos humanos no identificados.

II. NORMATIVA ESPAÑOLA EN MATERIA DE PROTECCIÓN DE DATOS

1. Antecedentes

En el plano de la legislación interna, se incide en que el punto de partida en materia de protección de datos se encuentra necesariamente constituido por el artículo 18.4 de la Constitución, que señala 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».*

Carente inicialmente de desarrollo legislativo, el mandato contenido en dicho precepto no se tradujo de modo directo en la promulgación de norma alguna que diera un tratamiento general a la materia hasta algunos años después, mediante la aprobación de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal, cuya finalidad era hacer frente a los riesgos que para los derechos de la personalidad podía suponer el acopio y tratamiento de datos por medios informáticos, con la idea de implantar mecanismos cautelares que previniesen las violaciones de la privacidad que pudieran resultar del tratamiento de la información.

Sin embargo, esta norma, de breve vigencia, quedó superada en pocos años bajo el impulso que para esta materia supuso la entrada en vigor de la Directiva 95/46/EC. La transposición de la Directiva a la legislación española debería haberse producido antes de la finalización del año 1998, cosa que no sucedió hasta finales de 1999, mediante la publicación de la LOPD, que derogó la LORTAD, y el posterior Real Decreto 1720/2007, de 21 de diciembre, por el que se aprobó su Reglamento de desarrollo.

En consonancia con el texto constitucional la Ley Orgánica 15/1999 tenía por objeto garantizar y proteger, en lo concerniente al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar, siendo de aplicación a los *«datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado»*.

Sin entrar en el detalle de la regulación contenida en esta norma por haber sido, a su vez, derogada por la LOPDGDD, la misma definía los datos de carácter personal como *«cualquier información concerniente a personas físicas identificadas o identificables»*, siendo reseñable, como elemento más significativo de su regulación en lo que se refiere a la actividad policial el hecho de consagrar un artículo, el 22, a los ficheros de las Fuerzas y Cuerpos de Seguridad, sometiendo al régimen general de la Ley aquellos que tuvieran fines administrativos, y a un régimen específico los que tuvieran finalidad policial, en los términos siguientes:

> *«1. Los ficheros creados por las Fuerzas y Cuerpos de Seguridad que contengan datos de carácter personal que, por haberse recogido para fines administrativos, deban ser objeto de registro permanente, estarán sujetos al régimen*

> *general de la presente Ley. 2. La recogida y tratamiento para fines policiales de datos de carácter personal por las Fuerzas y Cuerpos de Seguridad sin consentimiento de las personas afectadas están limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales, debiendo ser almacenados en ficheros específicos establecidos al efecto, que deberán clasificarse por categorías en función de su grado de fiabilidad.»*

Respecto a estos últimos también se contemplaba la posibilidad de recogida de datos de carácter personal especialmente protegidos, así como la de denegar a los interesados el ejercicio de los derechos de acceso, rectificación o cancelación en función de los peligros que pudieran derivarse para la defensa del Estado o la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones policiales.

Cabe resaltar que el análisis siguiente es limitado y no exhaustivo, si bien, los personas que se acerquen a esta materia tendrán que tener en cuenta otra normativa aplicable en virtud de las circunstancias, el ámbito concreto de aplicación y de las distintas regulaciones derivadas del reparto constitucional de competencias incorporado en nuestro ordenamiento jurídico[1].

2. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales

La Ley Orgánica 3/2018 es la norma a través de la que se adapta al ordenamiento jurídico español el RGPD, y constituye la norma nacional básica a través de la que se articula la protección de las personas físicas en relación con el tratamiento de datos personales, en su calidad de derecho fundamental protegido por el artículo 18.4 de la Constitución.

No obstante, desde la perspectiva de la actuación policial lo más significativo de esta norma no es tanto lo que regula como lo que queda fuera de la misma. Su artículo 2.2 excluye del ámbito de aplicación de la LOPDGDD los tratamientos que, a su vez, se encuentran excluidos del ámbito de aplicación del Reglamento general de protección de datos. Entre estos tratamientos a los que esta norma no es de aplicación se encuentran los realizados:

> *«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.»*

Estos tratamientos de datos se regirán por lo dispuesto en su legislación específica, si es que existe, y sólo supletoriamente por lo establecido en el Reglamento general de protección de datos y en la Ley Orgánica 3/2018.

[1] Vid. Ej. Ley 2/2004, de 25 de febrero, de Ficheros de Datos de Carácter Personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos, Ley 32/2010, de 1 de octubre, de la Autoridad Catalana de Protección de Datos o la Ley 1/2014, de 24 de junio, de Transparencia Pública de Andalucía.

Como se ha anticipado en el capítulo anterior, este tipo de tratamientos son específicamente objeto de regulación por la DDP, y su régimen jurídico es el previsto en la LOPDP. Temporalmente, y hasta la entrada en vigor de ésta, la Disposición transitoria cuarta de la Ley Orgánica 3/2018, mantuvo la vigencia del artículo 22 de la derogada LOPD, y sus disposiciones de desarrollo 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.

Lo expuesto no implica que esta Ley Orgánica no resulte en absoluto de aplicación a la actividad policial. Además de su ya aludida condición de norma supletoria, ésta pasa a ser de aplicación directa cuando los datos personales sean tratados para otros fines distintos de los expuestos, como puede suceder en relación con ficheros utilizados por autoridades policiales para fines administrativos, a menos que el tratamiento se efectúe como parte de una actividad relacionada con la prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales. Esta circunstancia puede generar dificultades prácticas en la actuación policial en la medida en la que en algunos casos pueden suscitarse dudas acerca de la naturaleza o la finalidad de determinados tratamientos, así como por la existencia de actividades de tratamiento que pueden tener una naturaleza hibrida, en los que coinciden o se superponen tanto finalidades administrativas como de prevención o investigación de infracciones penales.

Tampoco se encuentran incluidos dentro del ámbito de aplicación de esta Ley Orgánica los tratamientos sometidos a la normativa sobre protección de materias clasificadas, a los que se hará referencia más adelante, que se regirán por su normativa específica.

Por último, es importante señalar que, conforme recoge el artículo 22.6 de esta norma:

> *«El tratamiento de los datos personales procedentes de las imágenes y sonidos obtenidos mediante la utilización de cámaras y videocámaras por las Fuerzas y Cuerpos de Seguridad y por los órganos competentes para la vigilancia y control en los centros penitenciarios y para el control, regulación, vigilancia y disciplina del tráfico, se regirá por la legislación de transposición de la Directiva (UE) 2016/680, cuando el tratamiento tenga fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública. Fuera de estos supuestos, dicho tratamiento se regirá por su legislación específica y supletoriamente por el Reglamento (UE) 2016/679 y la presente ley orgánica.»*

Es decir, la LOPDGDD deriva a la LOPDP la definición del régimen jurídico de la utilización de cámaras y videocámaras policiales, cuando su uso tenga por finalidad la prevención, investigación, detección o enjuiciamiento de infracciones penales, la ejecución de sanciones penales, y la protección y prevención en materia seguridad pública, lo cual tiene implicaciones directas sobre la regulación contenida hasta el momento sobre la utilización de sistemas de grabación de imágenes y sonidos por las Fuerzas y Cuerpos de Seguridad para la protección de los derechos y libertades y para garantizar la seguridad ciudadana en la Ley Orgánica

4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos, que se estudiarán con mayor detalle al tratar el contenido de la LOPDP, así como en el capítulo cuarto del presente trabajo.

3. 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

Con esta Ley Orgánica se pretende lograr la protección y la libre circulación de los datos personales tratados con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas para la seguridad pública en la Unión Europea. Este nuevo marco jurídico supone el establecimiento de un sistema homogéneo encaminado a facilitar un intercambio ágil y dinámico de esta información entre los Estados miembros, terceros Estados y Organizaciones Internacionales. De resultas, se mejorará la cooperación y colaboración internacional, así como la protección de los datos personales de las personas físicas en este ámbito.

En otro orden de consideraciones, resulta importante poner de relieve que la Directiva que transpone esta norma se aprueba como respuesta a las crecientes amenazas para la seguridad en el contexto nacional e internacional, que tienen, en numerosos casos, un componente transfronterizo. Por esta razón, la cooperación internacional y la transmisión de información de carácter personal entre los servicios policiales y judiciales de los países implicados, se convierte en un objetivo ineludible. Los atentados terroristas de 2001 supusieron un punto de inflexión en la necesidad de reforzar la cooperación judicial y policial en la lucha contra el terrorismo. La posibilidad de compartir a tiempo la información operativa precisa, se erige en un requisito de eficacia en la lucha contra este tipo de amenazas.

El artículo 63 de la Directiva disponía que los Estados miembros adoptarán, a más tardar el 6 de mayo de 2018, las disposiciones legales, reglamentarias y administrativas necesarias para el cumplimiento de estos objetivos, circunstancia que, sin embargo, no ha tenido lugar en España hasta junio de 2021, manteniéndose entre tanto vigente el artículo 22 de la derogada Ley 15/1999, de 13 de diciembre, de protección de datos de carácter personal, relativo a los ficheros de las Fuerzas y Cuerpos de Seguridad. Este retraso dio lugar a la emisión de la Carta de Emplazamiento 2018/0164 por la Comisión Europea con fecha 20 de julio de 2018 y dirigida al Reino de España, por falta de transposición, y posteriormente al Dictamen motivado emitido por la Comisión Europea con fecha 24 de enero de 2019, que desembocaron en la Demanda formulada por la Comisión Europea ante el Tribunal de Justicia de la Unión Europea, de fecha 4 de septiembre de 2019, fruto de la cual el 25 de febrero de 2021 se condenó finalmente al Reino de España por el incumplimiento de sus obligaciones condenando a España al pago de una sanción económica consiste una suma a tanto alzado de 15 millones y medio de euros,

y una multa coercitiva diaria superior a los 89.500 euros, siendo la primera vez que se imponen ambas sanciones conjuntamente.

Esta ley consta de una exposición de motivos, sesenta y un artículos divididos en ocho capítulos, cinco disposiciones adicionales, una disposición derogatoria, una transitoria y doce disposiciones finales, y en consonancia con lo dispuesto en la Directiva que transpone, su principal objetivo es concretamente:

- Crear un marco regulador nacional en lo que respecta al tratamiento de los datos personales por parte de las autoridades competentes, con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública;
- Garantizar, en primer lugar, el pleno respeto de los derechos fundamentales y, muy especialmente, del derecho a la intimidad y del principio de proporcionalidad en el tratamiento de los datos. Dicho tratamiento estará avalado por una argumentación que justifique el despliegue de sus efectos. En segundo término, se pretende preservar las garantías necesarias para asegurar la legalidad, en particular, en lo que a protección de datos de carácter personal se refiere;
- Asegurar que el intercambio de datos personales por parte de las autoridades competentes españolas y de la Unión Europea, no quede restringido ni prohibido por motivos relacionados con la protección de las personas físicas, en lo que respecta al tratamiento de estos datos personales;
- Establecer un régimen sancionador específico que aporte una respuesta proporcionada a los eventuales incumplimientos.

Entre los elementos más sobresalientes de esta norma cabe enunciar someramente la inclusión de todas las obligaciones y medidas de seguridad establecidas para el responsable del tratamiento, entre las cuales se encuentra la obligación de llevar un registro de actividades de tratamiento y un registro de operaciones, así como una evaluación de impacto relativa a la protección de datos. A su vez, la ley orgánica regula toda operación o conjunto de operaciones que comprenda datos personales, ya sea de modo automatizado o no, y entre las que se incluye la recopilación; registro; organización; estructuración; almacenamiento, adaptación o modificación; recuperación; consulta; utilización; cotejo o combinación; limitación del tratamiento; y supresión o destrucción de datos.

Al hilo de estas cuestiones, resulta pertinente abundar en la forma del tratamiento en el ámbito de categorías especiales de datos personales, entre las que se encuentran categorías de uso frecuente por parte de las autoridades competentes. Es el caso de algunos datos genéticos (perfiles o identificadores obtenidos de ADN) y ciertos datos biométricos dirigidos a identificar de manera unívoca a una persona (datos dactiloscópicos, lofoscópicos, etiquetas descriptivas de voz, escritura, rasgos faciales, entre otros).

De la misma forma se regulan específicamente los sistemas de grabación de imágenes y sonido por las Fuerzas y Cuerpos de Seguridad, de conformidad con lo que dispone el artículo 22.6 de la LOPDGDD.

Entrando en el detalle de la regulación, el capítulo I, «Disposiciones generales», define el *«objeto»* de la ley orgánica, entendido como la regulación de la pro-

tección de los datos de carácter personal tratados por los órganos que a efectos de esta tengan la consideración de autoridades competentes. Asimismo, se exige que el tratamiento tenga fines de prevención, detección, investigación o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y prevención frente a las amenazas contra la seguridad pública. También se prevé que el intercambio de datos personales por parte de las autoridades competentes españolas en el interior de la Unión Europea, cuando el Derecho de la Unión Europea o la legislación española exijan dicho intercambio, no estará limitado ni prohibido por motivos relacionados con la protección de las personas físicas respecto al tratamiento de sus datos personales.

Las autoridades competentes, a efectos de esta Ley Orgánica, se definen como autoridades públicas con competencias legalmente encomendadas para la consecución de los fines específicos incluidos en el ámbito de aplicación. En concreto, serán autoridades competentes: las Fuerzas y Cuerpos de Seguridad; las autoridades judiciales del orden jurisdiccional penal y el Ministerio Fiscal; las Administraciones Penitenciarias; la Dirección Adjunta de Vigilancia Aduanera; el Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias; y la Comisión de Vigilancia de Actividades de Financiación del Terrorismo. Todo ello, sin perjuicio de que los tratamientos que se lleven a cabo por los órganos jurisdiccionales se rijan por lo dispuesto en esta Ley Orgánica, en la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, y en las leyes procesales penales.

Se excluyen expresamente del ámbito de aplicación ciertos tratamientos, como los realizados por las autoridades competentes para fines distintos de los cubiertos por la Ley Orgánica; los llevados a cabo por los órganos de la Administración General del Estado en el marco de las actividades comprendidas en el ámbito del capítulo II del título V del Tratado de la Unión Europea, en relación a la Política Exterior y de Seguridad Común; los derivados de una actividad no comprendida en el ámbito de aplicación del Derecho de la Unión Europea; y los sometidos a la normativa sobre materias clasificadas, entre los que explícitamente se consideran incluidos los tratamientos relativos a la Defensa Nacional. Con carácter general esta Ley Orgánica no se aplica a los tratamientos de datos de personas fallecidas, sin perjuicio de los derechos de acceso, rectificación o supresión por las personas vinculadas a ellos por razones familiares o de hecho.

Entre las definiciones que incorpora el capítulo I se deben destacar las de *«responsable de tratamiento»*, que es la autoridad competente que sola o conjuntamente con otras, determine los fines y medios del tratamiento de datos personales, y la de «encargado del tratamiento», como la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento.

El capítulo II se refiere a los principios de protección de datos cuya garantía corresponde al responsable del tratamiento. Estos principios se regulan en términos similares a lo establecido en el Reglamento General de Protección de Datos, aunque con algunas especialidades.

Se arbitra un régimen de colaboración con las autoridades competentes, conforme al cual, salvo cuando sea legalmente exigible la autorización judicial u otro tipo de garantías, las Administraciones públicas o cualquier persona física o jurídica están sujetas a la obligación de proporcionar a las autoridades judiciales, al

Ministerio Fiscal o a la Policía Judicial la información que les soliciten y que sea necesaria para la investigación o enjuiciamiento de infracciones penales o la ejecución de las penas y la información necesaria para la protección y prevención frente a un peligro real y grave para la seguridad pública. La petición de la Policía Judicial se deberá ajustar exclusivamente al ejercicio de las funciones que les son propias, y deberá efectuarse siempre de forma motivada, concreta y específica, dando cuenta en todo caso a la autoridad judicial y fiscal. Todo ello, con la prevención de que el interesado no será informado de la transmisión de sus datos, a fin de garantizar la investigación.

Se regulan también los plazos de conservación y de revisión de los datos de carácter personal tratados. Su conservación tendrá lugar sólo durante el tiempo necesario para cumplir con los fines previstos en el artículo 1, estableciéndose con carácter general un plazo máximo de conservación de veinte años, pudiendo acordar excepcionalmente el responsable del tratamiento la necesidad de conservar los datos por más tiempo cuando concurran factores como la existencia de investigaciones abiertas, delitos no prescritos, necesidad de protección de las víctimas u otras circunstancias motivadas que hagan necesaria su conservación para el cumplimiento de los fines del artículo 1. Adicionalmente, se impone al responsable del tratamiento la obligación de revisar, como máximo cada tres años, la necesidad de conservar, limitar o suprimir el conjunto de los datos personales contenidos en cada una de las actividades de tratamiento bajo su responsabilidad.

El responsable del tratamiento deberá, en la medida de lo posible, distinguir en su tratamiento de los datos, las diversas categorías de interesados, tales como los sospechosos, los condenados o sancionados, las víctimas o afectados y los terceros involucrados, así como también verificar la calidad de los datos personales, diferenciando si los datos tratados son datos basados en hechos o en apreciaciones. Se establecen las condiciones que determinan la licitud de todo tratamiento de datos de carácter personal; esto es, que sean tratados por las autoridades competentes; que resulten necesarios para los fines de esta ley orgánica; y que, en caso necesario y en cada ámbito particular, se especifiquen las especialidades por una norma con rango de ley que incluya unos contenidos mínimos.

En caso de transmisión de datos sujetos a condiciones específicas de tratamiento, dichas condiciones deberán ser respetadas por el destinatario de los mismos, en especial la prohibición de transmitirlos o de utilizarlos para fines distintos para los que fueron transmitidos. De igual modo, se exige que el tratamiento de categorías especiales de datos, como son los que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, la afiliación sindical, así como el tratamiento de datos genéticos o biométricos, y los datos relativos a la salud, la vida sexual o la orientación sexual, solo pueda tener lugar cuando sea estrictamente necesario y se cumplan ciertas condiciones. Por último, se prohíbe la adopción de decisiones individuales automatizadas, incluida la elaboración de perfiles en este ámbito, salvo que esté autorizado expresamente por una norma con rango de ley del ordenamiento jurídico español o por el Derecho de la Unión Europea.

Uno de los aspectos más significativos que aborda esta norma es el de la videovigilancia por las Fuerzas y Cuerpos de Seguridad, a la que se dedican los artículos 15 a 19 y que, sin derogar expresamente el régimen de la Ley Orgáni-

ca 4/1997, de 4 de agosto, la vacía de contenido en un elevado porcentaje. En este sentido, se dispone que la captación, reproducción y tratamiento de datos personales por las FCS, así como las actividades preparatorias, no se considerarán intromisiones ilegítimas en el derecho al honor, a la intimidad personal y familiar y a la propia imagen, a los efectos de la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen. Asimismo, previene que la instalación de sistemas de grabación de imágenes y sonidos deberá ser conforme al principio de proporcionalidad, y ajustarse, en su caso, a lo dispuesto en la Ley de Enjuiciamiento Criminal, así como a la legislación específica en materia de tráfico cuando se trate de un uso destinado al control, regulación, vigilancia y disciplina del tráfico.

Se regula la instalación de videocámaras fijas en las vías o lugares públicos, en cuyo caso el público será informado de manera clara y permanente de la existencia de estas videocámaras fijas, sin especificar su emplazamiento, así como de la autoridad responsable del tratamiento ante la que poder ejercer sus derechos, y se aborda también la utilización de dispositivos de toma de imágenes y sonido de carácter móvil, cuyo uso deberá estar autorizado por el Delegado o Subdelegado del Gobierno y, en su caso, por los órganos correspondientes de las comunidades autónomas con Cuerpos de Policía propios. En estos supuesto, las autorizaciones no se podrán conceder en ningún caso con carácter indefinido o permanente, debiendo otorgarse por el plazo adecuado a la naturaleza y las circunstancias derivadas del peligro o evento concreto, por un periodo máximo de un mes prorrogable por otro, con la previsión de que, en los casos de urgencia o necesidad inaplazable, será el responsable operativo de las FCS competentes el que podrá determinar su uso, siendo comunicada de inmediato tal actuación al Delegado o Subdelegado del Gobierno o autoridad competente de las comunidades autónomas.

En caso de que la grabación captara la comisión de hechos que pudieran ser constitutivos de infracciones penales, las FCS pondrán la cinta o soporte original de las imágenes y sonidos, en su integridad, a disposición judicial, a la mayor brevedad posible y, en todo caso, en el plazo máximo de setenta y dos horas desde su grabación; y si se captaran hechos que pudieran ser constitutivos de infracciones administrativas relacionadas con la seguridad pública, se remitirán al órgano administrativo competente, de inmediato, para el inicio del oportuno procedimiento sancionador. En todo caso, las grabaciones serán destruidas en el plazo máximo de tres meses desde su captación, salvo que estén relacionadas con infracciones penales o administrativas graves o muy graves en materia de seguridad pública, sujetas a una investigación policial en curso o con un procedimiento judicial o administrativo abierto. Por último, se establece la sujeción de las infracciones en relación con las actividades de videovigilancia sujetas a esta ley a lo dispuesto en la ley orgánica de régimen disciplinario correspondiente, sin perjuicio de las responsabilidades de orden penal a que pudiera haber lugar.

El capítulo III, regula los derechos de las personas, recogiendo en primer lugar un régimen general, que se refiere, en primer término, a las condiciones generales del ejercicio de los derechos, tales como la obligación exigible al responsable del tratamiento de facilitar la información correspondiente a los derechos del interesado de forma concisa, con un lenguaje claro y sencillo y de manera

gratuita; la información que debe ponerse a disposición del interesado, siendo algunos datos obligatorios en todo caso, y otros solo en casos concretos; se reconocen los derechos de acceso, rectificación, supresión y limitación, que facultan al interesado a conocer si se están tratando o no sus datos y, en caso afirmativo, acceder a cierta información sobre el tratamiento; a obtener la rectificación de sus datos si estos resultaran inexactos; a suprimirlos cuando fueran contrarios a lo dispuesto en la propia ley o cuando así lo requiera una obligación legal exigible al responsable; y a limitar el tratamiento, cuando el interesado ponga en duda la exactitud de los datos o estos datos deban conservarse únicamente a efectos probatorios o de seguridad. Estos derechos podrán ser ejercidos por el interesado directamente o, en determinados casos, a través de la autoridad de protección de datos, aunque pueden ser restringidos por ciertas causas tasadas, como cuando sea necesario para evitar que se obstaculice una investigación o se ponga en peligro la seguridad pública o la seguridad nacional.

La sección segunda de este capítulo establece un régimen especial para el ejercicio de los derechos de los interesados cuando los datos personales formen parte de investigaciones y procesos penales, conforme al cual se ejercerán con arreglo a las normas procesales penales, aplicándose la presente ley con carácter supletorio.

El capítulo IV, regula las obligaciones y responsabilidades del responsable y encargado del tratamiento de protección de datos. En primer lugar, se tratan las obligaciones generales del responsable del tratamiento en orden a la aplicación de las medidas técnicas y organizativas apropiadas para garantizar que el tratamiento se lleve a cabo de conformidad con la ley orgánica y la legislación sectorial aplicable, y que resulten conformes con los fines del tratamiento y los riesgos para los derechos y libertades de las personas físicas, debiendo garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que resulten necesarios para cada uno de los fines específicos del tratamiento. Se prevé el supuesto en que dos o más responsables del tratamiento determinen conjuntamente los objetivos y los medios de tratamiento, así como que una operación de tratamiento pueda ser llevada a cabo por encargados del tratamiento que actúan por cuenta del responsable, mediante un contrato u otro acto jurídico vinculante que observe las estipulaciones indicadas. Se obliga a que el encargado del tratamiento, así como a cualquier persona que actúe bajo la autoridad del responsable o del encargado del tratamiento y tenga acceso a datos personales, realice el tratamiento siguiendo únicamente instrucciones del responsable del tratamiento, a menos que esté obligado a hacerlo por disposición de la legislación española o del Derecho de la Unión Europea,

Cada responsable del tratamiento deberá conservar un registro de todas las actividades de tratamiento de datos personales realizadas bajo su responsabilidad, que incluya datos e información, tales como los datos de identificación y contacto del responsable del tratamiento, así como del delegado de protección de datos y, en su caso, del corresponsable, los fines del tratamiento, las categorías de interesados, entre otros datos, y también un registro de operaciones específicas de tratamiento en sistemas de tratamiento automatizado. El registro de operaciones constituye la pieza básica de este sistema, que comprende la recogida, alteración, consulta, comunicación y transferencias, entre otras operaciones, a los

efectos de verificar la legalidad del tratamiento, controlar el cumplimiento de las medidas y de las políticas de protección de datos, y garantizar la integridad y la seguridad de los datos personales en el ámbito de los procesos penales.

De igual modo, se prevén otra serie de obligaciones, como son la obligación de cooperación de los responsables y encargados del tratamiento con las autoridades de protección de datos; y la de evaluación del impacto del tratamiento, con carácter previo a este, cuando suponga un alto riesgo para los derechos y libertades de las personas físicas, lo que supone establecer una obligación que responde a un nuevo modelo de responsabilidad activa que exige una valoración previa del riesgo que pudiera generar el tratamiento de los datos de carácter personal para los interesados, para, a partir de dicha valoración, adoptar las medidas que procedan.

En materia de seguridad del tratamiento, se regulan las medidas técnicas y organizativas que de modo general deben aplicar los responsables y encargados del tratamiento para garantizar un nivel de seguridad adecuado, y las referidas específicamente al tratamiento automatizado, como el control de acceso a los equipamientos, el de los soportes de datos, el del almacenamiento, el de los usuarios y el control de acceso a los datos, entre otros, imponiendo, asimismo, el deber de notificación a la autoridad de protección de datos de cualquier violación de la seguridad que con carácter general, en caso de afectar a derechos y libertades de las personas físicas, deberá ser notificada al interesado, salvo en los supuestos expresamente previstos en la ley.

El Delegado de Protección de Datos se configura como el órgano o figura de asesoramiento y supervisión de los responsables de protección de datos, que podrá ser único para varias autoridades competentes y cuya designación será obligatoria salvo en relación con los tratamientos de datos con fines jurisdiccionales. En el caso de que se dispongan tratamientos que queden bajo distintos ámbitos de aplicación, con el fin de evitar disfunciones en las organizaciones de las autoridades competentes, se establece que la figura del delegado de protección de datos será única para todos ellos.

El capítulo V regula las transferencias de datos personales realizadas por las autoridades competentes españolas a un Estado que no sea miembro de la Unión Europea o a una organización internacional, y establece las condiciones que deberán cumplirse para que estas sean lícitas. Así, solo podrán realizarse estas transferencias cuando sean necesarias para los fines de esta ley orgánica, y cuando el responsable del tratamiento en el tercer país o en la organización internacional sea autoridad competente en relación con dichos fines. Asimismo, la autoridad competente del Estado miembro en el que se obtuvo el dato debe autorizar previamente esta trasferencia y las ulteriores que puedan tener lugar a otro tercer país u organización internacional.

En cuanto al tercer país no miembro de la Unión Europea o la organización internacional destinataria de la trasferencia, ésta deberá ser objeto de evaluación mediante una decisión de adecuación adoptada por la Comisión Europea a la vista de su nivel de protección de datos; o, en caso de ausencia de decisión de adecuación, cuando concurran determinadas garantías adecuadas que aprecie el responsable del tratamiento; y, en ausencia de ambas, cuando concurran algunas de las circunstancias excepcionales previstas en la propia Ley Orgánica, relacionada fundamentalmente con la necesidad de prevenir una amenaza inmediata y grave

y que la autorización previa no pueda conseguirse a su debido tiempo. En este caso las autoridades españolas informarán sin dilación a la autoridad responsable de conceder la citada autorización previa.

El capítulo VI, relativo a las autoridades de protección de datos, dispone que dichas autoridades sean la Agencia Española de Protección de Datos y las Agencias Autonómicas de Protección de Datos, en sus respectivos ámbitos competenciales. Asimismo, la Ley Orgánica recoge sus potestades y funciones, tanto de asesoramiento, supervisión y control, entre otras, como de investigación, incluyendo el acceso a todos los datos que estén siendo tratados por el responsable o el encargado del tratamiento, en los términos previstos por la legislación vigente. También se contempla la asistencia entre autoridades de protección de datos de los distintos Estados miembros.

En relación con las autoridades de protección de datos, cabe destacar que el capítulo VII, remite a la LOPDGDD, y en su caso a la legislación autonómica correspondiente, en relación con las reclamaciones que se formulen ante ellas. También se regulan aquellos supuestos en que los responsables o encargados del tratamiento, o la autoridad de protección de datos, incumplan esta Ley Orgánica y generen un daño o lesión en los bienes o derechos del interesado, estableciendo el régimen de responsabilidad patrimonial por daños sufridos por los interesados distinguiendo en función de si el responsable o encargado del tratamiento forma parte del sector público o es ajeno a él. Además, se contempla que los actos y resoluciones dictadas por la autoridad de protección de datos competente son susceptibles de recurso ante la jurisdicción contencioso-administrativa.

La ley orgánica contiene un régimen sancionador específico aplicable a los incumplimientos de las obligaciones previstas en la misma, al que se dedica el capítulo VIII. Los sujetos sobre los que recae la responsabilidad por las infracciones cometidas son los responsables de los tratamientos, los encargados de los tratamientos, los representantes de los encargados no establecidos en el territorio de la Unión Europea, así como el resto de las personas físicas o jurídicas obligadas por el contenido del deber de colaboración establecido en el capítulo II. Asimismo, se determinan las normas de conflicto para resolver los casos en los que un hecho pueda ser calificado con arreglo a dos o más normas, siempre que no constituyan infracciones al RGPD, ni a la LOPDGDD, y se tipifican las infracciones, que, en función de su gravedad, podrán ser leves, graves o muy graves. En general y de forma muy resumida, se consideran infracciones muy graves aquellas actuaciones que supongan vulneración de los derechos, principios y garantías establecidas en la ley, u obstrucción de la actividad inspectora de las autoridades competentes o incumplimiento de sus resoluciones; infracciones graves aquellas que sin incurrir en tales vulneraciones, incumplen las condiciones o circunstancias a las que se deben ajustar los tratamientos de datos, o supongan ausencia de adopción de medidas de seguridad apropiadas para aplicar de forma efectiva los principios de protección de datos; y leves la afectación leve de los derechos de los interesados por falta de diligencia, incumplimiento del principio de transparencia de la información o de la obligación de informar al interesado, así como la realización de notificaciones o comunicación de informaciones defectuosas o incompletas, entre otras.

Por su parte, entre las disposiciones finales son dignas de mención las relativas a la introducción de las modificaciones necesarias en la Ley Orgáni-

ca 1/1979, de 26 de septiembre, General Penitenciaria, para adecuarla a las previsiones de esta Ley Orgánica en relación con los tratamientos de datos para ejecución de la pena; la modificación de los artículos 235, 235 bis, 236 bis, 236 ter, 236 quáter, 236 quinquies, 236 sexies, 236 septies, 236 opties, 236 nonies, 236 decies y 560 de la Ley Orgánica 6/1985 de 1 de julio, del Poder Judicial, los artículos 12 y 14 de la Ley 50/1981, de 30 de diciembre, reguladora del Estatuto Orgánico del Ministerio Fiscal, y en el texto refundido de la Ley sobre Tráfico, Circulación de Vehículos a Motor y Seguridad Vial, aprobado por el Real Decreto Legislativo 6/2015, de 30 de octubre, para dar soporte legal específico a las matriculaciones por razones de Seguridad Nacional, carente hasta este momento de regulación específica y conforme a la cual, cuando concurran circunstancias que puedan afectar a la Seguridad Nacional, el Secretario de Estado de Seguridad podrá autorizar una nueva matrícula distinta de la inicialmente asignada. Este tipo de matrículas no serán públicas en el Registro General de Vehículos e, incluso en circunstancias excepcionales, podrá utilizarse una titularidad supuesta en el marco de la actuación de las FCS y del CNI en el tráfico jurídico.

4. Ley Orgánica 1/2020, de 16 de septiembre, sobre la utilización de los datos del Registro de Nombres de Pasajeros para la prevención, detección, investigación y enjuiciamiento de delitos de terrorismo y delitos graves

El Acuerdo de Schengen firmado el 14 de junio de 1985 se completó en 1990 con el Convenio de aplicación del Acuerdo de Schengen (CAAS) que creó el espacio Schengen mediante la abolición de los controles fronterizos dentro del Espacio Schengen, disposiciones comunes sobre visados y cooperación policial y judicial. El CAAS establece un requisito general para la cooperación policial y para que las autoridades policiales correspondientes intercambien información dentro de los límites de sus respectivos ordenamientos jurídicos nacionales, creándose el Sistema de Información de Schengen (SIS) en virtud de las disposiciones de su título IV, como medida destinada a compensar la ausencia de controles en las fronteras interiores de personas dentro del espacio Schengen mediante un instrumento de intercambio de información entre autoridades competentes. Actualmente se encuentra en funcionamiento el Sistema de Información de Schengen de segunda generación (SIS II), implantado en 26 Estados miembros de la Unión Europea, así como en otros cuatro países ajenos a la misma asociados a la cooperación Schengen: Islandia, Noruega, Suiza y Liechtenstein.

El SIS es un sistema de información a gran escala que permite a las autoridades competentes de los Estados Schengen introducir y consultar alertas sobre personas y objetos en relación con el control del espacio Schengen y cuya finalidad es garantizar la seguridad en dicho entorno, constituyendo un sistema tanto de control fronterizo como de cooperación policial y un soporte para la cooperación operativa entre autoridades policiales y autoridades judiciales en asuntos penales.

Desde finales de 2021 el marco normativo fundamental del SIS lo constituyen el Reglamento (UE) 2018/1860 del Parlamento Europeo y del Consejo, de 28 de noviembre de 2018, sobre la utilización del Sistema de Información de Schengen

para el retorno de nacionales de terceros países en situación irregular; complementado por el Reglamento (UE) 2018/1861 del Parlamento Europeo y del Consejo, de 28 de noviembre de 2018, relativo al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen (SIS) en el ámbito de las inspecciones fronterizas, por el que se modifica el Convenio de aplicación del Acuerdo de Schengen y se modifica y deroga el Reglamento (CE) n.° 1987/2006, y que se erige en la base jurídica para el SIS en todo lo referente a control de fronteras; y el Reglamento (UE) 2018/1862 del Parlamento Europeo y del Consejo, de 28 de noviembre de 2018, relativo al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen (SIS) en el ámbito de la cooperación policial y de la cooperación judicial en materia penal, por el que se modifica y deroga la Decisión 2007/533/JAI del Consejo, y se derogan el Reglamento (CE) 1986/2006 del Parlamento Europeo y del Consejo y la Decisión 2010/261/UE de la Comisión, que se configura como la norma esencial en relación con el funcionamiento del SIS en materia de cooperación policial y judicial.

Entre las medidas de control de fronteras puestas en marcha como consecuencia de la desaparición de las fronteras interiores se encuentra el sistema de información Avanzada de Pasajeros (API), que presenta grandes similitudes, aunque también importantes diferencias, con el sistema de Registro de Nombres de Pasajeros (PNR).

El sistema API, regulado en la Directiva 2004/82/CE del Consejo de 29 de abril de 2004, incorporado a nuestro ordenamiento a través la reforma del artículo 66 de la Ley Orgánica 4/2000, de 11 de enero, sobre derechos y libertades de los extranjeros en España y su integración social, y desarrollado por medio de la Resolución de 14 de febrero de 2007, por la que se determinan las rutas sobre las que se establecen obligaciones de información por parte de las compañías, empresas de transportes o transportistas, complementa lo establecido para el cruce de fronteras por parte del Convenio de Aplicación del Acuerdo de Schengen de 14 de junio de 1985, y tiene por objeto luchar contra la inmigración ilegal y mejorar el control fronterizo y de los flujos migratorios, estableciendo un sistema que regule las obligaciones de los transportistas aéreos que traen pasajeros al territorio de los Estados miembros de comunicar a estos los datos de las personas transportadas, acompañado de la posibilidad de imponer sanciones pecuniarias para el caso de incumplimiento de estas obligaciones por parte de los transportistas.

Las medidas contempladas en esta Directiva recogen las posibilidades de control previstas en el CAAS, que permiten aumentar los controles en las fronteras y disponer de tiempo suficiente para realizar un control fronterizo detallado y pormenorizado de cada uno de los pasajeros gracias a la transmisión de los datos de las personas transportadas a las autoridades encargadas de realizar los controles.

El tratamiento de datos personales por las autoridades de los Estados miembros en este contexto quedaba sujeto a la entonces vigente Directiva 95/46/CE, lo que se traducía en que, si bien resultaba legítimo tratar los datos de los pasajeros transmitidos a efectos de los controles fronterizos también lo era permitir su utilización como elemento de prueba en procedimientos destinados a la aplicación de las leyes y reglamentos relativos a la entrada y a la inmigración, incluidas sus disposiciones sobre la protección del orden público y la seguridad nacional. Cual-

quier otro tratamiento de datos incompatible con dichos fines habría resultado contrario a la Directiva 95/46/CE.

El artículo 66.1 de la LOEX indica que respecto de las rutas procedentes de fuera del espacio Schengen que determinen las autoridades españolas en atención a la intensidad de los flujos migratorios:

> *«A efectos de combatir la inmigración ilegal y garantizar la seguridad pública, toda compañía, empresa de transporte o transportista estará obligada, en el momento de finalización del embarque y antes de la salida del medio de transporte, a remitir a las autoridades españolas encargadas del control de entrada la información relativa a los pasajeros que vayan a ser trasladados, ya sea por vía aérea, marítima o terrestre, y con independencia de que el transporte sea en tránsito o como destino final, al territorio español.*
>
> *La información será transmitida por medios telemáticos, o, si ello no fuera posible, por cualquier otro medio adecuado, y será comprensiva del nombre y apellidos de cada pasajero, de su fecha de nacimiento, nacionalidad, número de pasaporte o del documento de viaje que acredite su identidad y tipo del mismo, paso fronterizo de entrada, código de transporte, hora de salida y de llegada del transporte, número total de personas transportadas, y lugar inicial de embarque...»*

Siguiendo literalmente lo previsto en artículo 6 de la Directiva 2004/82/CE en relación con el tratamiento de datos personales, la LOEX incorpora la previsión de que las autoridades encargadas del control de entrada guardarán los datos en un fichero temporal, borrándolos tras la entrada y en un plazo de veinticuatro horas desde su comunicación, salvo necesidades en el ejercicio de sus funciones. Los transportistas deberán haber informado de este procedimiento a los pasajeros, estando obligados a borrar los datos en el mismo plazo de veinticuatro horas.

Los usos a los que pueden destinarse esos datos se limitan a los fines legales de las autoridades encargadas de los controles de personas en las fronteras exteriores, aunque podrán utilizar asimismo a efectos policiales, con arreglo a la legislación nacional y respetando las disposiciones sobre protección de datos que actualmente, dado su carácter como fichero policial de naturaleza administrativa, viene constituido por el Reglamento (UE) 2016/679 general de protección de datos, y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Sin embargo, esta perspectiva esencialmente orientada al control de fronteras comenzó a reorientarse tras los atentados terroristas del 11-S en Estados Unidos. A partir de ese momento por parte de ese país se dicta una batería de leyes y normas diversas tendentes a reforzar la seguridad nacional. Entre ellas, la *«Aviation and Transport Security Act»*, de 19 de noviembre de 2001 y la *«Enhanced Border Security and Visa Entry Reform Act»*, de 14 de mayo de 2002, en cuya virtud, en aras a la persecución del terrorismo internacional, se obliga a todas las compañías dedicadas al transporte aéreo internacional de pasajeros, con vuelos con destino, origen o escala en Estados Unidos, a proporcionar acceso electrónico al Servicio de Aduanas y Protección de Fronteras del Departamento de Seguridad Interior estadounidense al registro electrónico de las compañías.

En el ámbito europeo la observancia de los requisitos exigidos por Estados Unidos ocasionaba ciertos problemas desde el punto de vista de la protección de datos personales, ya que ese país, pese a reconocer la privacidad en la Cuarta Enmienda de su Constitución, no reconoce con carácter general el derecho fundamental a la protección de los mismos, que se limita a aquellos casos en que existe un riesgo de abuso gubernamental en el trato de la información personal o respecto de sectores que almacenan información sensible. A ello se une la falta de tutela respecto de los datos de pasajeros que no son ciudadanos o residentes legales de los Estados Unidos.

Desde esta perspectiva facilitar este tipo de información a las autoridades de Estados Unidos constituía un debate en cuyos términos parece haber tenido considerable peso la condición de socio estratégico de Estados Unidos pese a que suponía una transferencia internacional que no se ajustaba plenamente a los criterios de la, entonces en vigor, Directiva 95/46/CE. Tras una serie de tentativas que llegaron hasta el Tribunal de Justicia de la Unión Europea, finalmente el 6 de noviembre de 2007, la Comisión adoptó la propuesta de Decisión marco del Consejo sobre utilización de datos del registro de nombres de los pasajeros con fines policiales, aunque la entrada en vigor el Tratado de Lisboa el 1 de diciembre de 2009, en cuya fecha la propuesta de la Comisión todavía no había sido aprobada por el Consejo, hizo que quedara obsoleta.

En este contexto político, la Comisión presentó una serie de elementos esenciales de la política de la Unión en esta materia en su Comunicación de 21 de septiembre de 2010 «Sobre el enfoque global de las transferencias de datos de los registros de nombres de los pasajeros (PNR) a los terceros países», en la que tomaba como punto de partida el sistema de información avanzada de pasajeros creado por la Directiva 2004/82/CE, teniendo en consideración el hecho de que las compañías aéreas ya recopilaban, trataban y almacenaban este tipo de información para sus usos estrictamente comerciales, por lo que no suponía imponer a estas obligaciones de recopilación de nuevos datos ni a los pasajeros la de proporcionar información adicional.

Fruto de estas iniciativas, y no sin considerable debate interno, tuvo lugar la aprobación el 27 de abril de 2016, de la Directiva (UE) 2016/681 del Parlamento Europeo y del Consejo, relativa a la utilización de datos del registro de nombres de los pasajeros (PNR) para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave, con un doble objetivo:

- Garantizar la seguridad, y proteger la vida y la seguridad de los ciudadanos.
- Crear un marco jurídico para la protección de los datos PNR en lo que respecta a su tratamiento por las autoridades competentes.

Por tanto, en relación con la operativa del sistema PNR, su finalidad es prevenir, detectar, investigar y enjuiciar delitos de terrorismo y otros delitos graves, para los que es fundamental que las compañías aéreas que realizan vuelos exteriores de la UE, estén sujetas a la obligación de transferir todos los datos PNR que recojan, incluidos los datos API, a las autoridades de los Estados miembros, facul-

tándose a éstos a ampliar esa obligación a las compañías aéreas que realizan vuelos interiores de la Unión Europea.

Los datos PNR deben transmitirse por parte de las compañías aéreas conforme a los protocolos definidos en la Decisión de Ejecución de la Comisión UE 2017/759, de 28 de abril de 2017, a una unidad única de información de pasajeros (UIP) designada en el Estado miembro de que se trate, y que en España es la Oficina Nacional de Información de Pasajeros (ONIP), integrada en la estructura orgánica del Centro de Inteligencia contra el Terrorismo y el Crimen Organizado (CITCO) de la Secretaría de Estado de Seguridad. Sus funciones únicas y exclusivas son la recogida de datos PNR, almacenarlos, tratarlos y transferir, en su caso, dichos datos o el resultado de su tratamiento a las autoridades competentes.

Los datos se envían en dos momentos distintos, el primero entre las cuarenta y ocho y las veinticuatro horas anteriores a la salida programada del vuelo, y el segundo una vez cerrado el vuelo, es decir, en el momento a partir del cual nadie puede entrar en el avión ni abandonarlo. Si durante el vuelo se produce alguna modificación en el destino, también deberá ser transmitida, y cuando resulte necesario acceder a los datos PNR para responder a una amenaza real y concreta en momentos distintos a los anteriores, caso por caso, las compañías aéreas también deberán transmitir dichos datos con carácter inmediato. La UIP cotejará los datos PNR con las distintas bases de datos disponibles y pertinentes a los efectos de la prevención, detección, investigación y enjuiciamiento de delitos de terrorismo y delitos graves, y tratará los datos de acuerdo con los criterios predeterminados. Estos tratamientos pueden ser compartidos con los órganos que se designen internamente por cada Estados miembros como autoridades competentes.

La DPNR fue objeto de transposición al ordenamiento español por medio de la Ley Orgánica 1/2020, de 16 de septiembre, sobre la utilización de los datos del Registro de Nombres de Pasajeros para la prevención, detección, investigación y enjuiciamiento de delitos de terrorismo y delitos graves que, tras una accidentada tramitación, entró en vigor el 17 de noviembre de 2020. En el ámbito de la Ley Orgánica, las autoridades competentes para solicitar o recibir datos PNR o el resultado del tratamiento de dichos datos por la UIP nacional (la ONIP), con el objetivo de seguir examinando dicha información o adoptar las medidas adecuadas para prevenir, detectar, investigar y enjuiciar delitos de terrorismo y delitos graves, son las Direcciones Generales de la Policía y de la Guardia Civil, el Centro Nacional de Inteligencia, la Dirección Adjunta de Vigilancia Aduanera y el Ministerio Fiscal, así como las autoridades competentes de las Comunidades Autónomas con competencias para la protección de personas y bienes y para el mantenimiento de la seguridad ciudadana y cuenten con un cuerpo de policía propio. No obstante, las peticiones serán debidamente motivadas, sin que se admitan peticiones masivas y no fundamentadas.

En el ámbito comunitario se contempla que cuando ello se considere necesario para la prevención, detección, investigación o enjuiciamiento de delitos de terrorismo o delitos graves, las UIP transmitan, cuando proceda y sin demora, los resultados del tratamiento de datos PNR a las de otros Estados miembros, para ulterior investigación. Transmisión e intercambio que también se puede realizar a través de Europol. La transferencia de datos a Europol se llevará a cabo electró-

nicamente y de forma motivada, siempre que entre dentro del ámbito de sus competencias y sea necesaria para el ejercicio de sus funciones.

En coherencia con las tensiones a las que dio lugar el largo proceso de gestación de la DPNR, el marco jurídico del sistema PNR contiene un extenso desarrollo de sus previsiones normativas para garantizar que el tratamiento de datos personales sea proporcional a los objetivos específicos de seguridad que persigue la Directiva. Para ello, en primer lugar, son frecuentes las referencias a que los tratamientos de datos efectuados en ejecución de esta normativa deben garantizar la protección de los derechos fundamentales y, en particular, el derecho a la intimidad y la protección de datos personales, imponiendo exigencias elevadas, conforme a la Carta de los Derechos Fundamentales de la Unión Europea, el Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (Convenio 108) y el Convenio para la protección de los derechos humanos y de las libertades fundamentales (CEDH).

En caso de que la UIP reciba datos PNR o el resultado de su tratamiento de la Unidad de otro Estado Miembro deberá proporcionar todos los datos pertinentes y necesarios a las autoridades correspondientes, tras una revisión individualizada. Asimismo, la UIP nacional tiene derecho a pedir de otro Estado miembro, mediante solicitud debidamente motivada para su valoración por éste, que le suministren los datos PNR que tengan almacenados siempre que no hayan sido despersonalizados, así como, si fuera necesario, el resultado de cualquier tratamiento de los mismos. En caso de que hayan sido despersonalizados la transmisión tendrá lugar conforme al derecho del Estado miembro de la UIP requerida. En el caso español, esto sólo es posible cuanto lo autorice la autoridad judicial o el titular de la Secretaría de Estado de Seguridad, y resulte necesario para la prevención, detección, investigación o enjuiciamiento de delitos de terrorismo.

Las transferencias de datos PNR a terceros países se permiten solo caso por caso y respetando plenamente lo establecido en la legislación de transposición de la DDP, que en nuestro caso es la LOPDP. Además, deberá tratarse de una transmisión de datos necesaria para los fines de esta ley orgánica, y el Estado receptor de los mismos solamente podrá transmitirlos, a su vez, a otro tercer Estado si cuenta para ello con la expresa autorización de la Unidad española. En todo caso, se garantizará que la transmisión y la utilización de datos PNR a terceros Estados mantengan unos estándares y garantías como los previstos en la ley orgánica, lo que en la práctica resulta difícil de acreditar.

Teniendo plenamente en cuenta los principios de la jurisprudencia del Tribunal de Justicia de la Unión Europea, la aplicación de la normativa sobre PNR debe garantizar el pleno respeto de los derechos fundamentales y el derecho a la intimidad, así como el principio de proporcionalidad, debiendo respetarse escrupulosamente los objetivos de necesidad y proporcionalidad, así como la necesidad de proteger los derechos y libertades en la lucha contra el terrorismo y la delincuencia grave. Entre los derechos fundamentales objeto de protección se mencionan expresamente el derecho a la protección de datos personales y el derecho a la no discriminación, señalándose que no debe tomarse ninguna decisión que pudiera tener efectos jurídicos adversos para una persona o afectarle gravemente en razón únicamente del tratamiento automatizado de datos PNR.

Es preciso mencionar el régimen jurídico al que está sujeto el tratamiento de datos de carácter personal realizado en el marco de esta normativa, que pese a la similitud de los datos con respecto a los del sistema API, es sustancialmente distinto en atención a la finalidad perseguida. Dada la heterogeneidad de los actores, y las finalidades y legitimaciones de los responsables del tratamiento, el sistema legal que converge sobre los sujetos obligados y los tratamientos derivados de las obligaciones impuestas a los mismos, es decir a las compañías aéreas o entidades de gestión de reservas que recopilan estos datos para su actividad comercial, se regirán por lo dispuesto en la propia Ley Orgánica 1/2020, así como en RGPD, y por la LOPDGDD. Sin embargo, como así se recoge en el artículo 11 de la LOPNR, por parte de las autoridades competentes en nuestro país se estará a lo dispuesto en la LOPDP.

Respecto a las peculiaridades propias de estos tratamientos recogidas en la LOPNR, cabe recoger que la recogida y uso de datos sensibles, como los relativos a salud, origen étnico, ideología u orientación sexual, queda terminantemente prohibida, debiendo borrarse inmediatamente en caso de recibirse, lo que supone una diferencia notable con la LOPDP, que sí permite su tratamiento cuando sea estrictamente necesario.

El período durante el cual deben conservarse los datos PNR debe ser el necesario, y debe ser proporcional a las finalidades de prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y los delitos graves. En este sentido, en garantía del derecho a la intimidad de los sujetos afectados los datos PNR facilitados por los sujetos obligados serán conservados durante cinco años a contar desde su transmisión. Cumplido ese plazo serán suprimidos definitivamente, sin perjuicio de su utilización por parte de las autoridades competentes que los hayan recibido y que los estén utilizando en el marco de un asunto concreto a efectos de prevenir, detectar, investigar o enjuiciar delitos de terrorismo o delitos graves. Sin embargo, transcurridos seis meses desde la recepción de los datos PNR, aquella información que permita la identificación directa del pasajero será despersonalizada mediante enmascaramiento, y solo se permitirá el acceso a la totalidad de la misma previa aprobación por la autoridad judicial o por el titular de la Secretaría de Estado de Seguridad.

Adicionalmente, es obligatorio conservar la documentación relativa a los sistemas y procedimientos de tratamiento y disponer de un registro de las operaciones de recogida, consulta, transferencia y supresión de los datos a efectos de la verificación de su legalidad, de autocontrol, así como para garantizar adecuadamente la integridad y seguridad del tratamiento; así como comunicar al interesado y a la autoridad nacional de control cualquier violación de los datos personales que dé lugar a un elevado riesgo para la protección de los mismos o afecte negativamente a la intimidad del interesado.

Asimismo, con el fin de garantizar la eficiencia y un alto nivel de protección de datos, se exige a los Estados miembros que garanticen que una autoridad nacional de control independiente y, en particular, un responsable de la protección de datos, sea responsable de asesorar y de supervisar el modo en que se tratan los datos PNR. Esta previsión se desarrolla en el artículo 8.1 de la propia Ley Orgánica, conforme al cual:

> *«1. La UIP designará una persona como responsable de protección de los datos PNR que velará por que se adopten las medidas oportunas para contro-*

lar el tratamiento de estos datos y porque se apliquen las garantías en materia de protección de datos. El responsable de protección de datos actuará como punto de contacto único, al que cualquier interesado tendrá derecho a dirigirse para todas las cuestiones relativas al tratamiento de sus datos PNR.»

Aunque se confiere a este responsable una relevancia y protección del máximo nivel a través de su recogida en una norma con rango de Ley Orgánica, nada obsta para que esta función hubiera recaído en la figura ya existente del Delegado de Protección de Datos. Sin embargo, en la transposición de la Directiva a nuestro ordenamiento, dentro del margen de decisión que la misma dejaba a las Estados miembros, se optó por crear una figura específica, carente de tal carácter, con funciones limitadas a la supervisión de este fichero e integrado orgánica y funcionalmente en el CITCO, siendo susceptible de debate si con ello se refuerzan efectivamente las garantías en materia de protección de datos en relación con el uso y supervisión de este fichero.

Por último, tanto la Directiva como su Ley Orgánica de transposición incorporan un régimen sancionador específico. Particularmente, se prevén sanciones pecuniarias para las compañías aéreas y sujetos obligados que infrinjan de alguna forma sus obligaciones relativas a la transmisión de datos, y sobre los que recae directamente la responsabilidad por las infracciones cometidas en este sentido, tanto por acción como por omisión, pudiendo calificarse como muy graves, graves o leves. En general, se consideran como muy graves aquellas infracciones que consisten en omisiones o incumplimientos que implican un riesgo grave para la seguridad ciudadana, la vida o la integridad física de las personas; graves cuando no exista dicho riesgo; y leves algunas conductas residuales que se refieren a determinados aspectos de menor trascendencia o que supongan incumplimiento a cualquier otra obligación derivada de la normativa que no constituya infracción grave o muy grave. Todos los incumplimientos relativos a un mismo vuelo se consideran una única infracción. Por su parte, el responsable de tratamiento responderá conforme prevé la Ley Orgánica 7/2021, que en su condición de autoridad competente sólo prevé para el mismo sanciones de apercibimiento.

Las características de este sistema se pueden estudiar a nivel práctico en lo publicitado en el Registro de Actividades de Tratamiento del Ministerio del Interior que se puede consultar en la página web del Departamento establecida al efecto[2].

5. Anteproyecto de Ley Orgánica por la que se establecen normas que faciliten el uso de información financiera y de otro tipo para la prevención, detección, investigación o enjuiciamiento de infracciones penales, por el que se transpone la Directiva (UE) 2019/1153 del Parlamento Europeo y del Consejo, de 20 de junio de 2019

El anteproyecto materializa la transposición a nuestro ordenamiento jurídico de la Directiva (UE) 2019/1153 del Parlamento Europeo y del Consejo, de 20 de

[2] http://www.interior.gob.es/web/servicios-al-ciudadano/participacion-ciudadana/proteccion-de-datos-de-caracter-personal/tutela-de-los-derechos#registro

junio de 2019, que deroga la Decisión 2000/642/JAI del Consejo de 17 de octubre de 2000 relativa a las disposiciones de cooperación entre las unidades de información financiera de los Estados miembros para el intercambio de información. La lucha contra cualquier forma grave de delincuencia, en particular, contra el fraude financiero, el blanqueo de capitales y la financiación del terrorismo, constituye una prioridad para la Unión Europea. En consecuencia, facilitar el intercambio y el acceso a la información financiera resulta imprescindible al objeto de prevenir, detectar, investigar o enjuiciar, no sólo la comisión de estas acciones delictivas, sino también, respecto de otros delitos de especial gravedad.

Fruto de esa preocupación, y como continuación a otras Directivas a través de las que la Unión Europea ha buscado reforzar la lucha contra la criminalidad organizada, se adoptó la Directiva (UE) 2018/843 del Parlamento Europeo y del Consejo, de 30 de mayo de 2018, por la que se modifica la Directiva (UE) 2015/849 relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, y por la que se modifican las Directivas 2009/138/CE y 2013/36/UE. Esta Directiva pretendía reforzar la coordinación y colaboración, a todos los niveles, de las Unidades de Inteligencia Financiera (UIF) de los Estados miembros, a las que compete recoger y analizar la información financiera que reciben con la finalidad de establecer vínculos entre las transacciones sospechosas y la actividad delictiva subyacente, a fin de prevenir y luchar contra el blanqueo de capitales y la financiación del terrorismo.

En España la función de Unidad de Inteligencia Financiera es asumida por el Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias (SEPBLAC), al que, conforme a la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo, los sujetos obligados (entidades financieras, de servicios de inversión, aseguradoras, promotores inmobiliarios, notarios, registradores, casinos, casas de compraventa de joyas o metales preciosos, abogados, etc.) están obligados a comunicar cualquier hecho u operación respecto al que tengan indicio o sospecha de que está relacionado con el blanqueo de capitales o la financiación del terrorismo, así como determinadas operaciones sujetas a comunicación sistemática. Para la realización de sus funciones el SEPBLAC es el encargado de tratamiento del denominado Fichero de Titularidades Financieras, del cual es responsable la Secretaría de Estado de Economía, y al que las entidades de crédito deben declarar la apertura o cancelación de cuentas corrientes, cuentas de ahorro, depósitos y de cualquier otro tipo de cuentas de pago, así como los contratos de alquiler de cajas de seguridad. La declaración contendrá, en todo caso, los datos identificativos de los titulares, representantes o autorizados y cualesquiera otras personas con poderes de disposición. La información de los productos debe incluir en todo caso su numeración, el tipo de producto y las fechas de apertura y de cancelación. En el caso de las cajas de seguridad se incluirá la duración del periodo de arrendamiento, pudiendo determinarse reglamentariamente otros datos de identificación que deban ser declarados.

El último paso de este proceso ha sido la aprobación de la Directiva (UE) 2019/1153 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, por la que se establecen normas destinadas a facilitar el uso de información financiera y de otro tipo para la prevención, detección, investigación o enjuiciamiento de infracciones penales y por la que se deroga la Decisión 2000/642/JAI del Consejo, objeto de trans-

posición por este anteproyecto, que pretende ampliar el acceso a los registros centralizados de cuentas bancarias y de pagos, que en España es el citado Fichero de Titularidades Financieras, garantizando acceso directo e inmediato a esa información, cuya dificultad de acceso por parte de las autoridades policiales, entre otras, provoca en la práctica retrasos significativos, susceptibles de afectar a las investigaciones penales. Para ello, la DDFIN prevé el acceso directo de las autoridades competentes a los registros nacionales centralizados de cuentas bancarias o a los sistemas de recuperación de datos, autorizando igualmente el acceso indirecto a Europol a través de las unidades nacionales de los Estados miembros, ya que a pesar de que Europol no lleve a cabo investigaciones penales, sí apoya las acciones de los Estados miembros.

Salvando los cambios que pueda sufrir durante su tramitación, actualmente el anteproyecto se compone de 14 artículos divididos en cuatro capítulos, dos disposiciones adicionales y ocho disposiciones finales, y tiene como principales objetivos, conforme a lo dispuesto en la Directiva que transpone:

- Facilitar el uso directo e inmediato de la información financiera para prevenir, detectar, investigar o enjuiciar delitos graves.
- Reforzar la seguridad, mejorar el enjuiciamiento de los delitos financieros, luchar contra el blanqueo de capitales y prevenir los delitos fiscales, mejorando el acceso a la información por parte de las Unidad de Información Financiera (UIF) y las autoridades públicas responsables de la prevención, detección, investigación o enjuiciamiento de delitos graves, potenciando su capacidad para llevar a cabo investigaciones financieras y mejorar la cooperación entre ellas.
- Con el fin de aumentar la seguridad jurídica y la eficacia operativa, busca establecer normas que refuercen la capacidad de las UIF para compartir información financiera y análisis financieros con las autoridades competentes designadas con respecto a todas las infracciones penales graves.
- Establecer un marco jurídico claramente definido que permita a la UIF solicitar los datos almacenados por las autoridades competentes designadas a fin de poder prevenir, detectar y luchar contra el blanqueo de capitales, los delitos antecedentes conexos y la financiación del terrorismo de manera efectiva.
- Establecer un mecanismo claro y robusto que proteja los datos personales y su tratamiento.

La norma designa a las autoridades competentes a los efectos de la misma, que son las Autoridades judiciales del orden jurisdiccional penal, el Ministerio Fiscal, las Fuerzas y Cuerpos de Seguridad, y la Dirección Adjunta de Vigilancia Aduanera de la Agencia Estatal de Administración Tributaria; así como, en su caso, las Oficinas de Recuperación de Activos. Los hechos delictivos por los que se tiene derecho a acceder a la información objeto de la norma, son únicamente los delitos graves, entendidos como las formas de delincuencia enumeradas en el anexo I del Reglamento (UE) 2016/794 del Parlamento Europeo y del Consejo, de 11 de mayo de 2016, así como los *«delitos antecedentes conexos del delito de blanqueo»*, en los términos de la Directiva (UE) 2018/1673, de 23 de octubre de 2018, relativa a la lucha contra el blanqueo de capitales.

Asimismo, en los capítulos I y II se describe de manera específica, el tipo y alcance de la información susceptible de acceso e intercambio para lograr un equilibrio entre la eficiencia y la protección de los datos personales:

- Por un lado, la información financiera contenida en el Fichero de Titularidades Financieras: la información sobre cuentas bancarias y de pago, cajas de seguridad, así como otros productos declarables. Información que incluirá la información de los productos a declarar incluyendo la numeración que los identifique, el tipo de producto y las fechas de apertura y de cancelación o la duración del periodo de arrendamiento en el caso de cajas de seguridad, los datos identificativos de los titulares de estos productos, de sus titulares reales, de los representantes o autorizados y de cualesquiera otras personas con poderes de disposición, así como cualquier otro dato que se declare en el Fichero.
  El acceso y la consulta se llevarán a cabo para la prevención, detección, investigación o enjuiciamiento de un delito grave o para apoyar una investigación penal en relación con un delito grave, incluida la identificación, localización e inmovilización de los activos relacionados con dicha investigación. El acceso y la consulta al Fichero de Titularidades Financieras, sólo podrán ser realizada, caso por caso, por personal específicamente designado y autorizado para realizar estas tareas a través de los puntos únicos de acceso establecidos por las autoridades competentes.
  En línea con la finalidad de la Directiva, la Disposición final primera del anteproyecto modifica el artículo 43 de la Ley 10/2010 al objeto de eliminar el requisito de autorización judicial previa para acceder al Fichero de Titularidades Financieras.
- Por otro, los «análisis financieros»: que son los resultados del análisis operativo y estratégico que haya llevado a cabo el SEPBLAC, que responderá a aquellas solicitudes de información financiera que obren en su poder o de análisis financieros realizados, a la mayor brevedad posible. Estas peticiones deberán ser motivadas en atención a las circunstancias del caso, y resultar necesarias para la prevención, detección, investigación o enjuiciamiento de delitos graves, pudiendo ser denegadas en determinadas circunstancias, como resultar desproporcionadas, y esta información sólo puede utilizarse para otros fines distintos de los autorizados con previo consentimiento del SEPBLAC.
  En el mismo sentido y a sensu contrario, el SEPBLAC también puede pedir, en el ámbito de sus competencias, colaboración de las autoridades competentes para recibir información o datos de naturaleza policial que estén a su disposición.

El intercambio de información con otros Estados miembros de la Unión Europa por parte de las autoridades competentes está expresamente permitido, de acuerdo con los mecanismos vigentes de cooperación policial y judicial. A tal fin, las autoridades competentes españolas podrán intercambiar la información financiera o los análisis financieros con una autoridad competente de otro Estado miembro previa solicitud motivada, cuando resulte necesario para el ejercicio de sus competencias

respecto a la prevención, detección y la lucha contra el blanqueo de capitales, los delitos antecedentes conexos y la financiación del terrorismo. La misma colaboración puede mantenerse con Europol siempre que las solicitudes estén debidamente motivadas, se mantengan en su ámbito de competencia y se dirijan al desempeño de sus funciones, materializándose a través de la Unidad Nacional de Europol.

Dado el carácter sensible de los datos financieros, el capítulo IV de esta norma establece una serie de disposiciones suplementarias relativas al tratamiento y protección de los datos personales derivadas de la aplicación de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales; de 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; así como de la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo. Hay que tener en cuenta que el tratamiento de los datos personales contenidos en el Fichero de Titularidades Financieras por el Servicio Ejecutivo de la Comisión se regirá por la Ley Orgánica 3/2018, sin perjuicio del régimen aplicable a las autoridades competentes en relación con los tratamientos realizados por éstas en cumplimiento de las finalidades previstas en el presente anteproyecto.

En este ámbito, lo más significativo en cuanto a la debida garantía de los derechos de los interesados consiste en el establecimiento de un mecanismo específico de protección de la información que se cede, creándose un sistema de doble registro de las operaciones, aplicable tanto al SEPBLAC como a las autoridades competentes, a través del que éstas quedan perfectamente trazadas, y que se conservarán durante un período de cinco años después de su creación. Los datos de estos registros de operaciones se utilizarán solamente a efectos de comprobar la legalidad del tratamiento y controlar el cumplimiento de las medidas y de las políticas de protección de datos, así como garantizar la integridad y la seguridad de los datos personales, que estarán a disposición de la autoridad de protección de datos competente a solicitud de ésta.

Este Anteproyecto fue aprobado por el Consejo de Ministros el 22 de junio de 2021 para su tramitación y, con fecha 24 de febrero de 2022, el Consejo de Estado emitió por unanimidad el Dictamen Nº 1159/2021 sobre el mismo.

El contenido de dicho dictamen, tras un análisis exhaustivo del mandato de contenido en la DDFIN y de los requisitos constitucionales de nuestro ordenamiento, es bastante clarificador en cuanto a la posibilidad de un acceso directo e inmediato a los registros centralizados de cuentas bancarias y otros productos sin el requisito de una decisión judicial anterior.

Concluye el Consejo de Estado que el acceso al fichero de titularidades financieras por las autoridades competentes sin necesidad de previa autorización judicial resulta proporcionado con la exigencia de garantizar la seguridad pública y respetuoso con el derecho fundamental a la intimidad proclamado en el artículo 18.1 de la CE.

Sin perjuicio de como resulte la tramitación urgente de la norma (Exp.121/000099), este proyecto parece otro buen instrumento para la lucha contra algunas de las principales amenazas contra la seguridad pública como serían el terrorismo, el crimen organizado y el blanqueo de capitales.

6. Tratamiento de datos personales en el ámbito procesal penal

Como se apuntó previamente, la LOPDP, es de aplicación a la protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, no obstante, su artículo 2.2. señala que *«el tratamiento de los datos personales llevado a cabo con ocasión de la tramitación por los órganos judiciales y fiscalías de las actuaciones o procesos de los que sean competentes, así como el realizado dentro de la gestión de la Oficina judicial y fiscal, en el ámbito del artículo 1,se regirá por lo dispuesto en la presente Ley Orgánica, sin perjuicio de las disposiciones de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial , las leyes procesales que le sean aplicables y, en su caso, por la Ley 50/1981, de 30 de diciembre, por la que se regula el Estatuto Orgánico del Ministerio Fiscal. Las autoridades de protección de datos a las que se refiere el capítulo VI no serán competentes para controlar estas operaciones de tratamiento.»*

Esta circunstancia, en la práctica, supone la existencia de un régimen específico en la materia en el ámbito del proceso penal, lo que, sin perjuicio de la aplicación de la Ley Orgánica 7/2021 a los tratamientos de datos policiales con fines de investigación, tiene implicaciones directas en cuanto a la determinación del marco jurídico de protección de datos personales aplicable a aquellas actuaciones policiales que hayan sido incorporadas a las actuaciones judiciales o del Ministerio Fiscal, que quedarán sujetas a este régimen.

De hecho, en el artículo 26, perteneciente a la segunda sección de su capítulo III «Derechos de las personas», que el ejercicio de los derechos de información, acceso, rectificación, supresión y limitación respecto al tratamiento de los datos en los procesos penales se llevará a cabo de conformidad con lo dispuesto en la Ley Orgánica 6/1985 de 1 de julio, del Poder Judicial, en las normas procesales, y, en su caso, en la Ley 50/1981, de 30 de diciembre, reguladora del Estatuto Orgánico del Ministerio Fiscal.

Esta extensión al Ministerio Fiscal es una de las novedades más importantes de esta nueva regulación y tiene la finalidad de en la LOPJ todo lo relativo a la protección de datos respecto al tratamiento de datos con fines jurisdiccionales.

Hay que recordar que, por su propia naturaleza, la actuación de la Policía Judicial está orientada al esclarecimiento de los delitos y a aportar elementos probatorios al proceso penal. El artículo 120.1 de la Constitución proclama el carácter público de las actuaciones judiciales, aunque *«con las excepciones que prevean las leyes de procedimiento»*. En este sentido el artículo 301 de la Ley de Enjuiciamiento Criminal dice que *«las diligencias del sumario serán reservadas y no tendrán carácter público hasta que se abra el juicio oral, con las excepciones determinadas en la presente Ley»*. El sumario, y por extensión toda investigación criminal, tiene siempre carácter secreto en lo que al conocimiento general se refiere, sin necesidad de que el juez de instrucción acuerde específicamente dicho secreto, con objeto de evitar interferencias externas en el desarrollo de la investigación que puedan comprometer su desarrollo.

La LOPJ, distingue entre los tratamientos de datos realizados en el marco de la actividad jurisdiccional y aquellos que tiene lugar fuera de la misma. En relación con los primeros, se establece que el acceso a las resoluciones judiciales u

otras actuaciones procesales por quienes no son parte en el procedimiento y acrediten un interés legítimo y directo, podrá llevarse a cabo previa disociación, anonimización u otra medida de protección de los datos de carácter personal que las mismos contuvieren y con pleno respeto al derecho a la intimidad, a los derechos de las personas que requieran un especial deber de tutela o a la garantía del anonimato de las víctimas o perjudicados, cuando proceda.

Respecto a las partes procesales, el artículo 302 de la Ley de Enjuiciamiento Criminal indica que:

> *«las partes personadas podrán tomar conocimiento de las actuaciones e intervenir en todas las diligencias del procedimiento. No obstante, si el delito fuere público, podrá el Juez de Instrucción, a propuesta del Ministerio Fiscal, de cualquiera de las partes personadas o de oficio, declararlo, mediante auto, total o parcialmente secreto para todas las partes personadas,...».*

Esta modalidad de secreto no debe prolongarse más tiempo del estrictamente necesario para asegurar el resultado de la instrucción, con el plazo máximo de un mes, prorrogable por periodos iguales.

Conforme a la LOPJ, los Jueces y Magistrados, los Fiscales y los Letrados de la Administración de Justicia, conforme a sus competencias, podrán adoptar las medidas que sean necesarias para la supresión de los datos personales de las resoluciones y de los documentos a los que puedan acceder las partes durante el proceso siempre que no sean necesarios para garantizar el derecho a la tutela judicial efectiva, sin que, en ningún caso, pueda producirse indefensión. Los datos personales que las partes y los profesionales que los representan conocen a través del proceso deberán ser tratados por éstas de conformidad con la normativa general de protección de datos. Obligación que también incumbe a cualquier otra persona que intervenga en el procedimiento.

En el ámbito de la jurisdicción penal, el tratamiento de los datos personales llevado a cabo con ocasión de la tramitación por los órganos judiciales y fiscalías de los procesos o diligencias de los que sean competentes, así como el realizado dentro de la gestión de la Oficina judicial y fiscal, se regirá por lo dispuesto en la Ley Orgánica 7/2021, sin perjuicio de las especialidades establecidas en las leyes procesales, en la LOPJ y el EOMF.

Un ejemplo ilustrativo, entre otros muchos que podrían seleccionarse, de tratamiento de datos personales regulado por la Ley de Enjuiciamiento Criminal lo constituye la figura del agente encubierto, previsto en el artículo 282 bis de la misma, conforme al cual y junto a los aspecto operativos de su actuación, se determina que la identidad supuesta será otorgada por el Ministerio del Interior por el plazo de seis meses prorrogables por períodos de igual duración, así como que la resolución por la que se acuerde será reservada y deberá conservarse fuera de las actuaciones con la debida seguridad, debiendo consignar el nombre verdadero del agente y la identidad supuesta con la que actuará en el caso concreto. Identidad que, si así se acuerda por resolución judicial motivada, podrá mantenerse por los agentes policiales cuando testifiquen en el proceso, remitiendo a este respecto a la Ley Orgánica 19/1994, de 23 de diciembre, de protección a testigos y peritos en causas criminales, que prevé la posibilidad de que motivadamente se puedan

adoptar las medidas necesarias para preservar la identidad de los testigos y peritos, su domicilio, profesión y lugar de trabajo.

La LOPJ también establece que no será necesario obtener el consentimiento del interesado para que se pueda proceder al tratamiento de los datos personales en el ejercicio de la actividad jurisdiccional, ya sean éstos facilitados por las partes o recabados a solicitud de los órganos competentes, sin perjuicio de lo dispuesto en las normas procesales para la validez de la prueba. En estos supuestos el ejercicio de los derechos de información, acceso, rectificación, supresión y limitación se tramitarán conforme a la normativa citada específicamente aplicable a estos tratamientos, debiendo ejercitarse ante los órganos judiciales, fiscalías u Oficina judicial que conocen del procedimiento, y deberán resolverse por quien tenga la competencia atribuida en la normativa orgánica y procesal. En todo caso se denegará a los interesados el acceso a los datos objeto de tratamiento con fines jurisdiccionales cuando las diligencias procesales en que se haya recabado la información sean o hayan sido declaradas secretas o reservadas.

Respecto a las operaciones de tratamiento efectuadas con fines jurisdiccionales, corresponderán al Consejo General del Poder Judicial y a la Fiscalía General del Estado, en el ámbito de sus respectivas competencias, las funciones de supervisión del cumplimiento de la normativa de protección de datos; y las competencias que corresponden a la autoridad de protección de datos personales con fines jurisdiccionales serán ejercidas respecto del tratamiento de los mismos realizado por Juzgados y Tribunales por la Dirección de Supervisión y Control de Protección de Datos del Consejo General del Poder Judicial y la Unidad de Supervisión y Control de Protección de Datos que ejercerá las competencias que corresponden a la autoridad de protección de datos con fines jurisdiccionales sobre el tratamiento de los mismos realizado por el Ministerio Fiscal.

Resulta indispensable, en todo caso, la lectura de los preceptos previamente citados: artículos 235, 235 bis, 236 bis, 236 ter, 236 quáter, 236 quinquies, 236 sexies, 236 septies, 236 opties, 236 nonies, 236 decies y 560 de la LOPJ, los artículos 12 y 14 del EOMF.

7. Tratamientos de datos sometidos a la normativa de materias clasificadas

Los tratamientos sometidos a la normativa sobre materias clasificadas, entre los que se encuentran los relativos a la Defensa Nacional no se encuentran sujetos a la LOPDGDD, estando asimismo expresamente excluidos del ámbito de aplicación de la LOPDP. La normativa básica en esta materia en España viene constituida por la Ley 9/1968, de 5 de abril, de Secretos Oficiales, modificada por la Ley 48/1978, 7 de octubre, cuya reforma o sustitución se encuentra actualmente en estudio por el Gobierno, y por el Decreto 242/1969, de 20 de febrero, por el que se desarrollan las disposiciones de aquella. No obstante, dada la obsolescencia de este marco regulatorio, el mismo se encuentra completado por las Normas dictadas por la Autoridad Nacional para la Protección de la Información Clasificada.

La publicidad y la transparencia constituyen la norma básica en relación con la actividad ordinaria del Estado democrático, y así aparece recogido en diversos

artículos de la Constitución que, sin embargo, en su artículo 105.b) también excluye de la misma aquello que *«afecte a la seguridad y defensa del Estado, la averiguación de los delitos y la intimidad de las personas»*. En este sentido, la propia Ley 9/1968, pese a su carácter preconstitucional, reconoce el principio general de *«la publicidad de la actividad de los Órganos del Estado»*, aunque para expresar inmediatamente la *«necesidad de imponer limitaciones, cuando precisamente de esa publicidad puede derivarse perjuicio para la causa pública, la seguridad del mismo Estado o los intereses de la colectividad nacional»*.

¿Qué materias tienen la condición de secretas y se encuentran sujetas a esta norma? En primer lugar, aquellas que, sin necesidad de ser expresamente clasificadas, estén así declaradas por una ley. Y en segundo lugar, podrán ser declarados materias clasificadas los asuntos, actos, documentos, informaciones, datos y objetos, cuyo conocimiento por personas no autorizadas pueda dañar o poner en riesgo la seguridad del Estado o comprometa los intereses fundamentales de la Nación en materia referente a la defensa nacional, la paz exterior o el orden constitucional. Se trata, por tanto, de materias de la más variada índole, que no tiene porqué contener necesariamente datos de carácter personal. Éstas serán calificadas en las categorías de secreto y reservado en atención a su importancia y al grado de protección que requieran, correspondiendo su clasificación y desclasificación, en función de sus competencias, al Consejo de Ministros y sus miembros, a los Jefes de Misiones Diplomáticas de España en el extranjero, y al Jefe del Estado Mayor de la Defensa.

Siempre que ello sea posible, la autoridad encargada de la calificación indicará el plazo de duración de ésta, así como el personal que puede tener acceso a la información y las formalidades y limitaciones que sean necesarias para el cumplimiento de esta clasificación. Las personas facultadas para tener acceso a una materia clasificada quedan obligadas a cumplir con las medidas y prevenciones de protección que se hayan establecido, correspondiendo a las Autoridades anteriormente señaladas conceder en sus respectivos ámbitos las autorizaciones para acceso a las mismas. Se prevé que la infracción de las normas sobre información clasificada contenidas en esta ley pueda ser sancionada penalmente, como delitos de descubrimiento y revelación de secretos e informaciones relativas a la defensa nacional, y disciplinariamente en el ámbito administrativo como falta muy grave, sin mayor concreción, por lo que debe acudirse al régimen disciplinario que en cada caso proceda.

La información o material clasificado deben estar debidamente inventariados y registrados, y su custodia y uso exige la existencia de instalaciones específicas de seguridad para su almacenaje y protección, a los cuales no pueden tener acceso personas que no hayan sido autorizadas para ello, regulándose la existencia de Servicios de Protección de Materias Clasificadas en cada Departamento que disponga de este tipo de información, para asegurar su adecuado tratamiento.

La Ley 9/1968 señala que la calificación de secreto o reservado no impedirá el cumplimiento de los trámites de audiencia, alegaciones, notificaciones directas a los Interesados, en la forma establecida en la legislación de procedimiento administrativo, sin perjuicio de la eventual aplicación de las sanciones previstas en caso de violación del secreto por parte de los interesados. Asimismo, contempla que compete a la autoridad encargada de la calificación señalar los procedimientos para determinar, periódicamente, la conveniencia de la reclasificación o desclasificación de aquel material, y se establecen normas para la destrucción o eli-

minación del material clasificado. El Decreto 242/1969 también crea la figura de la Autoridad Nacional para la Protección de la Información Clasificada (ANPIC), cuyo máximo responsable es el Secretario de Estado Director del CNI, y a la que corresponde velar por el cumplimiento de las normas sobre materias clasificadas, autorizar la creación de servicios de protección de información, y determinar las personas concretas autorizadas a acceder a la información clasificada. La ANPIC desarrolla sus funciones a través de la Oficina Nacional de Seguridad. A su vez, en cada Departamento ministerial que disponga de este tipo de información existirá un Servicio de Protección de Materias Clasificadas con la finalidad de asegurar el adecuado tratamiento de las materias clasificadas en su ámbito.

Al objeto de determinar las personas concretas autorizadas a acceder a la información clasificada, la ANPIC, previa solicitud del organismo del que dependen estas personas y la acreditación de la «necesidad de conocer», emite las correspondientes habilitaciones personales de seguridad, de una validez inicial de cinco años, prorrogables, sin las cuales no se puede manejar la información clasificada al amparo de la Ley 9/1968, de suerte que la mera posesión de un cargo oficial no implica autorización para acceder a la misma, pudiendo darse el caso de que la habilitación no se conceda por valorarse que puede existir algún riesgo de seguridad. La ANPIC también elabora las Normas de la Autoridad Nacional para la Protección de la Información Clasificada, en las cuales se define la estructura nacional de protección de la información clasificada; y se imparten normas de seguridad relativas al personal a través de la regulación del procedimiento de concesión de la habilitación personal de seguridad; de medidas específicas de seguridad física de las zonas en las que se custodia información clasificada; de seguridad de la información (clasificación, registro, distribución, transmisión, control, destrucción, archivo...); de seguridad en los sistemas de información y comunicaciones; y seguridad industrial.

De la regulación contenida en la Ley 9/1968 es de señalar, por una parte, que no establece una relación de materias clasificadas, sino la exigencia de una determinación genérica de su importancia, en base a la cual «podrá» procederse a su clasificación, aunque los Tribunales entienden que debe tratarse de una información relevante o trascendente y haber una relación directa entre el conocimiento de la misma y un peligro grave y cierto para la seguridad y defensa del Estado; y por otra, su carácter parcial, puesto que reconoce la posibilidad de existencia de materias clasificadas a través de otras normas, a cuyo respecto cabe hacer mención, como ejemplo de atribución legal de carácter secreto, sin la previa clasificación, a la información derivada del CNI, regulado en la Ley 11/2002, de 6 de mayo, que por imperativo del artículo 5.1 de su norma reguladora tiene el carácter de información clasificada como secreto. Otro tanto cabe decir de las obligaciones derivadas de la Ley Orgánica 19/1994, de 23 de diciembre, de protección a testigos y peritos en causas criminales, que también imponen medidas de secreto y confidencialidad en el tratamiento de la información. Igualmente, es significativa la ausencia de definición de unos requisitos legales mínimos de seguridad para la información clasificada; la indeterminación de las personas que están autorizadas a conocer dicha información, que dependerá de la naturaleza de la misma; o la falta de un mecanismo o procedimiento específico para la hipotética revisión de la conveniencia de la desclasificación de documentos o su reclasificación, más allá de un criterio de oportunidad en el caso concreto.

También en materia de infraestructuras críticas, de acuerdo con el artículo 4 del Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas, el Catálogo Nacional de Infraestructuras Estratégicas tiene, conforme a lo dispuesto en la legislación vigente en materia de secretos oficiales, la calificación de secreto, conferida por Acuerdo de Consejo de Ministros de 2 de noviembre de 2007, calificación que comprende, además de los datos contenidos en el propio Catálogo, los equipos, aplicaciones informáticas y sistemas de comunicaciones inherentes al mismo, así como el nivel de habilitación de las personas que pueden acceder a la información en él contenida. En este caso corresponde al Ministerio del Interior, a través de la Secretaría de Estado de Seguridad, la responsabilidad de clasificar una infraestructura como estratégica, así como de incluirla en el mencionado Catalogo.

Por su relevante significación en el ámbito de la actividad policial hay que destacar que, en ejecución de la excepción al derecho de información pública recogida en el artículo 105 b) de la Constitución y conforme a lo previsto en la Ley 9/1968, haciendo uso de la competencia que a tal efecto le atribuye el artículo 4 de esta ley, el Consejo de Ministros, mediante sendos acuerdos de 16 de febrero de 1996, y 6 de junio de 2014, otorgó con carácter genérico la clasificación de secreto, respectivamente, a la estructura, organización, medios y técnicas operativas utilizadas por las Fuerzas y Cuerpos de Seguridad del Estado en la lucha antiterrorista y contra la delincuencia organizada, así como sus fuentes y cuantas informaciones o datos puedan revelarlas. Es de señalar que, sin perjuicio de la interpretación extensiva que en un momento dado pueda hacerse de su texto, objetivamente estos acuerdos no cubren los ficheros ni los tratamientos de datos personales contenidos en los mismos realizados en el ámbito de la lucha contra estas formas de criminalidad, cuyo ámbito natural, en principio, debe ser el de 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.

Otra cuestión a tener en consideración es el hecho de que la Ley 9/1968 sólo contempla dos niveles de clasificación: secreto y reservado. Sin embargo, al margen de lo previsto en su texto existen otros niveles de reserva utilizados con habitualidad en la Administración para proteger determinadas informaciones cuya difusión puede afectar a los intereses públicos que en puridad, por su falta de anclaje normativo, no entran en el concepto de información clasificada, que se definen como «confidencial» o «difusión limitada» y que, conforme a las normas de la ANPIC pueden ser declarados por los Ministros, Secretarios de Estado y Subsecretarios de los distintos Departamentos, por el Jefe del Estado Mayor de la Defensa y por los de los tres Ejércitos. Tomados en conjunto, hacen que el sistema se corresponda con la escala de cuatro niveles de seguridad que se utilizan por la OTAN en el ámbito militar y por la mayor parte de los socios internacionales de España, aunque con cierta inconsistencia en cuanto a las distintas denominaciones y equivalencias entre cada uno de ellos, que pueden traducirse en problemas en materia de cooperación internacional.

Existen, además, otros ámbitos de información no clasificada formalmente que, sin embargo, tienen limitada su difusión pública y que pueden afectar en mayor o menor medida a la actividad policial. En este sentido, no se puede olvidar

que la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información y buen gobierno busca reforzar la transparencia en la actividad pública, garantizando el acceso a la información y estableciendo obligaciones de publicidad que deben ser objeto de cumplimiento por los responsables públicos. Sin embargo, una de las excepciones a la obligación de suministrar información, prevista en el artículo 14 de esta norma, que permite limitar el derecho de acceso es que el mismo suponga un perjuicio a la seguridad pública. En todo caso, la aplicación de los límites debe ser justificada y proporcionada a su objeto y finalidad de protección y atenderá a las circunstancias del caso concreto, especialmente a la concurrencia de un interés público o privado superior que justifique el acceso.

8. Tratamientos de datos sometidos a la normativa penitenciaria

El artículo 4 de la LOPDP, atribuye a las *«Administraciones Penitencias»* la consideración de autoridades competentes a los fines prevenidos en la misma. Cuestión nada baladí puesto que establece un régimen novedoso en relación con que previamente se recogía en su normativa específica.

La disposición final primera de esta norma introduce un nuevo artículo 15 bis en la Ley Orgánica 1/1979, de 26 de septiembre, General Penitenciaria, que establece:

> *«Artículo 15 bis. Tratamientos de datos de carácter personal.*
>
> *1. Admitido en el establecimiento un interno, se procederá a verificar su identidad personal, efectuando la reseña alfabética, dactilar y fotográfica, así como a la inscripción en el libro de ingresos y a la apertura de un expediente personal relativo a su situación procesal y penitenciaria, respecto del que se reconoce el derecho de acceso. Este derecho sólo se verá limitado de forma individualizada y fundamentada en concretas razones de seguridad o tratamiento.*
>
> *2. El tratamiento de los datos personales de los internos se regirá por lo previsto en la Ley Orgánica de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales. Los datos personales de categorías especiales que no figuren en el apartado anterior se podrán tratar con el consentimiento del interesado. Sólo se prescindirá de dicho consentimiento cuando sea estrictamente necesario y se efectúe con las garantías adecuadas para proteger el derecho a la protección de datos de los interesados, atendiendo al tipo de datos que se traten y a las finalidades de los distintos tratamientos dirigidos a la ejecución de la pena.*
>
> *3. Igualmente se procederá al cacheo de su persona y al registro de sus efectos, retirándose los enseres y objetos no autorizados.*
>
> *4. En el momento del ingreso se adoptarán las medidas de higiene personal necesarias, entregándose al interno las prendas de vestir adecuadas que precise, firmando el mismo su recepción.»*

La introducción de este precepto viene a solventar la problemática derivada de la circunstancia de que la regulación de un derecho fundamental tuviese lugar a través de un instrumento reglamentario, como ocurría con el contenido del Ca-

pítulo III del Real Decreto 190/1996, de 9 de febrero, por el que se aprueba el Reglamento Penitenciario.

Este capítulo recoge en sus artículos 6 a 9 lo siguiente:

«Artículo 6. Limitación del uso de la informática penitenciaria.

1. Ninguna decisión de la Administración penitenciaria que implique la apreciación del comportamiento humano de los reclusos podrá fundamentarse, exclusivamente, en un tratamiento automatizado de datos o informaciones que ofrezcan una definición del perfil o de la personalidad del interno.

2. La recogida, tratamiento automatizado y cesión de los datos de carácter personal de los reclusos contenidos en los ficheros se efectuará de acuerdo con lo establecido en la legislación sobre protección de datos de carácter personal y sus normas de desarrollo.

3. Las autoridades penitenciarias responsables de los ficheros informáticos penitenciarios adoptarán las medidas de índole técnica y organizativa necesarias para garantizar la seguridad de los datos de carácter personal en ellos contenidos, así como para evitar su alteración, pérdida, tratamiento o acceso no autorizado, y estarán obligadas, junto con quienes intervengan en cualquier fase del tratamiento automatizado de este tipo de datos, a guardar secreto profesional sobre los mismos, incluso después de que haya finalizado su relación con la Administración penitenciaria.

4. La Administración penitenciaria podrá establecer ficheros de internos que tengan como finalidad garantizar la seguridad y el buen orden del establecimiento, así como la integridad de los internos. En ningún caso la inclusión en dicho fichero determinará por sí misma un régimen de vida distinto de aquél que reglamentariamente corresponda.

Artículo 7. Recogida y cesión de datos de carácter personal de los internos.

1. Cuando los datos de carácter personal de los reclusos se recojan para el ejercicio de las funciones propias de la Administración penitenciaria no será preciso el consentimiento del interno afectado, salvo en los relativos a su ideología, religión o creencias.

2. Tampoco será preciso el consentimiento del recluso afectado para ceder a otras Administraciones públicas, en el ámbito de sus respectivas competencias, los datos de carácter personal contenidos en los ficheros informáticos penitenciarios que resulten necesarios para que éstas puedan ejercer sus funciones respecto de los internos en materia de reclutamiento para la prestación del servicio militar, servicios sociales, Seguridad Social, custodia de menores u otras análogas.

3. También se podrán ceder datos de carácter personal contenidos en los ficheros informáticos penitenciarios sin previo consentimiento del afectado cuando la cesión tenga por destinatarios al Defensor del Pueblo o institución análoga de las Comunidades Autónomas que ejerzan competencias ejecutivas en materia penitenciaria, al Ministerio Fiscal o a los Jueces o Tribunales, en el ejercicio de las funciones que tienen atribuidas, así como cuando se trate de cesión de datos de carácter personal relativos a la salud de los reclusos por motivos de urgencia o para realizar estudios epidemiológicos.

4. Las transferencias internacionales de datos de carácter personal contenidos en los ficheros informáticos penitenciarios se efectuarán en los supuestos de prestación de auxilio judicial internacional, de acuerdo con lo establecido en los tratados o convenios en los que sea parte España.

Artículo 8. Datos penitenciarios especialmente protegidos.

1. No obstante lo dispuesto en el artículo anterior, los datos de carácter personal de los reclusos relativos a opiniones políticas, a convicciones religiosas o filosóficas, al origen racial y étnico, a la salud o a la vida sexual, que hayan sido recabados para formular los modelos individualizados de ejecución o los programas de tratamiento penitenciarios, sólo podrán ser cedidos o difundidos a otras personas con el consentimiento expreso y por escrito del recluso afectado o cuando por razones de interés general así lo disponga una Ley.

2. Cuando se soliciten de la Administración Penitenciaria este tipo de datos especialmente protegidos por medio de representante del recluso, deberá exigirse, en todo caso, poder especial y bastante otorgado por el mismo en el que conste expresamente su consentimiento para que su representante pueda tener acceso a dichos datos personales del recluso.

Artículo 9. Rectificación y conservación de los datos.

1. Los reclusos podrán solicitar de la Administración penitenciaria la rectificación de sus datos de carácter personal contenidos en los ficheros informáticos penitenciarios que resulten inexactos o incompletos. De la rectificación efectuada se informará al interesado en el plazo máximo de dos meses desde su solicitud, así como al cesionario o cesionarios, en el supuesto de que los datos incorrectos hubiesen sido objeto de cesión previa.

2. Los datos de carácter personal de los reclusos contenidos en los ficheros informáticos penitenciarios no serán cancelados cuando, ponderados los intereses en presencia, concurran razones de interés público, de seguridad y de protección de los derechos y libertades de terceros, así como cuando posean un valor intrínseco de carácter histórico y estadístico a efectos de investigación.»

Como presupuesto específico resulta oportuno mencionar asimismo el artículo 215 que viene a clarificar el estatus de los datos e informaciones contenidas en la historia clínica y la información sanitaria de las personas internas en los centros penitenciarios. Este precepto fija que los datos integrados en la historia clínica individual tendrán carácter confidencial, debiendo quedar correctamente archivados y custodiados, siendo únicamente accesibles para el personal autorizado de la organización.

En el marco de la Secretaría General de Instituciones Penitenciarias cobra especial relevancia la profusión de circulares, instrucciones y ordenes relacionadas con la protección de datos que pueden ser consultados en sus repositorios web.

III. BREVE ESTUDIO ESPECÍFICO DE OTROS CONCEPTOS BÁSICOS EN EL MARCO DE LA LEY ORGÁNICA 7/2021

En el contexto de los tratamientos de datos personales realizados en el ámbito de la LOPDP, existen determinados conceptos que, por su relevancia y singularidad, merecen un trato individualizado.

1. Deber de colaboración

Sin perjuicio del contenido del artículo 18 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, del artículo 142 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, del artículo 7 de la Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana y de varios presupuestos contenidos en la LECRIM, la LOPDP incluye, en su artículo 7, un deber específico de colaboración con las autoridades competentes, en el contexto del ejercicio de las competencias a las que se refiere la Ley, cuyo incumplimiento puede ser constitutivo de una infracción administrativa, sin perjuicio de otras responsabilidades en las que se pueda incurrir. En concreto, señala que las Administraciones públicas, así como cualquier persona física o jurídica, proporcionarán a las autoridades judiciales, al Ministerio Fiscal o a la Policía Judicial los datos, informes, antecedentes y justificantes que les soliciten y que sean necesarios para la investigación y enjuiciamiento de infracciones penales o para la ejecución de las penas. La petición de la Policía Judicial se deberá ajustar exclusivamente al ejercicio de las funciones que en este sentido les encomienda la legislación, y está sujeta a los requisitos de que deberá efectuarse siempre de forma motivada, concreta y específica, dando cuenta en todo caso a la autoridad judicial y fiscal. Se exceptúan aquellos casos en los que legalmente sea exigible la autorización judicial para recabar los datos de que se trate.

En estos supuestos, a fin de garantizar la actividad investigadora, el interesado no será informado de la transmisión de sus datos a las autoridades competentes, ni de haber facilitado el acceso a los mismos por dichas autoridades de cualquier otra forma. Con el mismo propósito, los sujetos a los que el ordenamiento jurídico imponga este deber específico de colaboración con las autoridades competentes, no informarán al interesado de la transmisión de sus datos a dichas autoridades, ni de haber facilitado el acceso a los mismos por dichas autoridades de cualquier otra forma, en cumplimiento de sus obligaciones específicas.

Como puede apreciarse este deber de colaboración incluye en parte una restricción directa y legal de los derechos de los interesados que hace necesaria que la fundamentación y motivación de las peticiones de tratamiento sea completa y correcta.

La misma obligación de colaboración, y sujeta a las mismas condiciones, existe respecto de las restantes autoridades competentes definidas en la Ley Orgánica 7/2021. En el caso de otras autoridades competentes, las Administraciones públicas, así como cualquier persona física o jurídica, proporcionarán los datos, informes, antecedentes y justificantes a las autoridades competentes que los soliciten, siempre que estos sean necesarios para el desarrollo específico de sus mi-

siones para la prevención, detección e investigación de infracciones penales y para la prevención y protección frente a un peligro real y grave para la seguridad pública. La petición de la autoridad competente deberá ser concreta y específica y contener la motivación que acredite su relación con los indicados supuestos.

2. Plazos de conservación

Como se apuntó anteriormente en este texto, el artículo 8 de la LOPDP regula el plazo de conservación de los datos personales tratados al amparo de esta norma, así como la figura a la que corresponde la toma de decisiones a este respecto. De este modo, el responsable del tratamiento, que es la autoridad competente que sola o conjuntamente con otras determina los fines y medios del tratamiento de datos personales, determinará que la conservación de los datos personales tenga lugar sólo durante el tiempo necesario para cumplir con los fines para los que se han recabado.

Éste deberá revisar la necesidad de conservar, limitar o suprimir el conjunto de los datos personales contenidos en cada una de las actividades de tratamiento bajo su responsabilidad, como máximo cada tres años, atendiendo especialmente en cada revisión a la edad del afectado, el carácter de los datos y a la conclusión de una investigación o procedimiento penal. Para evitar que el responsable de tratamiento tenga que estar constantemente sometido a la obligación de revisar la necesidad de conservación de datos, se establece que, si es posible, este proceso se hará mediante el tratamiento automatizado apropiado.

Con carácter general, el plazo máximo para la supresión de los datos será de veinte años, salvo que concurran determinados factores que hacen incompatible aplicar dicho plazo como serían la existencia de investigaciones abiertas o delitos que no hayan prescrito, la no conclusión de la ejecución de la pena, reincidencia, necesidad de protección de las víctimas u otras circunstancias motivadas que hagan necesario el tratamiento de los datos para el cumplimiento de los fines de la Ley.

3. Calidad de los datos personales en el marco policial

La LOPDP recoge en su artículo 10 la obligación del responsable de tratamiento de verificar la calidad de los datos personales. En este sentido, se le impone la responsabilidad de establecer, en la medida de lo posible, una distinción entre los datos personales basados en hechos y los basados en apreciaciones personales.

Por su parte, las autoridades competentes adoptarán todas las medidas razonables para garantizar que los datos personales que sean inexactos, incompletos o no estén actualizados, no se transmitan ni se pongan a disposición de terceros, y en toda transmisión de datos se trasladará al mismo tiempo la valoración de su calidad, exactitud y actualización. En la medida de lo posible, en todas las transmisiones de datos personales se añadirá la información necesaria para que la autoridad competente receptora pueda valorar hasta qué punto son exactos, completos y fiables, y en qué medida están actualizados. Igualmente, la autoridad competente transmisora, en la medida en que sea factible, controlará la calidad de los datos personales antes de transmitirlos o ponerlos a disposición de terceros.

Se prevé que en caso de observarse que los datos personales transmitidos son incorrectos o que se han transmitido ilegalmente, estas circunstancias se pongan en conocimiento del destinatario sin dilación indebida. En tal caso, los datos deberán rectificarse o suprimirse, o el tratamiento deberá limitarse de conformidad con lo previsto a tal efecto en la propia Ley.

4. Mecanismo de decisión individual

Con objeto de salvaguardar los derechos fundamentales y la seguridad jurídica de los ciudadanos frente a actuaciones potencialmente arbitrarias de los poderes públicos basadas exclusivamente en el resultado de operaciones algorítmicas, el artículo 14 de la LOPDP prohíbe de forma expresa las decisiones basadas únicamente en un tratamiento automatizado, incluida la elaboración de perfiles, que produzcan efectos jurídicos negativos para el interesado o que le afecten significativamente, salvo que se autorice expresamente por una norma con rango de ley o por el Derecho de la Unión Europea. La norma habilitante del tratamiento deberá establecer las medidas adecuadas para salvaguardar los derechos y libertades del interesado, incluyendo el derecho a obtener la intervención humana en el proceso de revisión de la decisión adoptada.

Las decisiones basadas en un tratamiento automatizado a las que se refiere el apartado anterior no se podrán basar en las categorías especiales de datos personales salvo que se hayan tomado las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado. A este respecto, el artículo 13 considera categorías especiales de datos personales aquellos que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas o la afiliación sindical, así como el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, los datos relativos a la salud o a la vida sexual o a la orientación sexual de una persona física.

También se prohíbe la elaboración de perfiles que den lugar a una discriminación de las personas físicas sobre la base de las anteriores categorías especiales de datos personales.

5. Obligaciones del responsable del tratamiento y corresponsabilidad. Encargados de tratamiento

De acuerdo con los conceptos que recoge la propia Ley Orgánica, el responsable del tratamiento es *«la autoridad competente que sola o conjuntamente con otras, determine los fines y medios del tratamiento de datos personales; en caso de que los fines y medios del tratamiento estén determinados por el Derecho de la Unión Europea o por la legislación española, dichas normas podrán designar al responsable del tratamiento, o bien los criterios para su nombramiento»*. Y el encargado de tratamiento es *«la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento»*.

Es obligación del responsable del tratamiento, tomando en consideración la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como los nive-

les de riesgo para los derechos y libertades de las personas físicas, aplicar las medidas técnicas y organizativas apropiadas para garantizar que el tratamiento de datos personales se lleve a cabo de conformidad con la Ley Orgánica 7/2021 y con lo previsto en la legislación sectorial y en sus normas de desarrollo. Tales medidas se revisarán y actualizarán cuando resulte necesario. Entre las medidas mencionadas se incluirá la aplicación de las oportunas políticas de protección de datos, cuando sean proporcionadas en relación con las actividades de tratamiento.

La norma permite que puedan existir dos o más responsables del tratamiento que determinen conjuntamente los objetivos y los medios de tratamiento. En este caso serán considerados *«corresponsables del tratamiento»*. Los corresponsables del tratamiento, salvo que sus responsabilidades hayan sido previstas por una norma, establecerán, de modo transparente y de mutuo acuerdo, a través del instrumento oportuno, sus respectivas responsabilidades en el cumplimiento de la Ley Orgánica, en particular, en lo referido al ejercicio de los derechos del interesado y a las obligaciones de cada uno de ellos en el suministro de la información que debe ponerse a disposición de aquel, contemplada en el artículo 21 y relativa a su propia identificación; los datos de contacto del delegado de protección de datos, en su caso; los fines del tratamiento; el derecho a presentar una reclamación ante la autoridad de protección de datos competente; y al derecho a solicitar del responsable del tratamiento el acceso a los datos personales del interesado y su rectificación, supresión o la limitación de su tratamiento.

La concreción de las responsabilidades de los corresponsables se realizará atendiendo a las actividades que efectivamente desarrolle cada uno de los corresponsables del tratamiento.

Respecto al encargado de tratamiento, se trata de una figura necesaria cuando una operación de tratamiento vaya a ser llevada a cabo por cuenta y bajo el mandato o decisión de un responsable del tratamiento, y podrá ser una persona física o jurídica, de naturaleza privada o pública. A su vez, el encargado del tratamiento no podrá recurrir a otro encargado sin la autorización previa por escrito del responsable del tratamiento.

Resulta imperativa la lectura las Guías de la AEPD que fijan los conceptos y obligaciones de los responsables y encargados de tratamiento, que, con los matices estudiados, resultan de aplicación a nuestro ámbito específico.

A modo de ejemplo, se consideran de gran utilidad:

- Guía del Reglamento General de Protección de Datos para responsables de tratamiento[3].
- Directrices para la elaboración de contratos entre responsables y encargados del tratamiento[4].
- Orientaciones para prestadores de servicios de 'Cloud Computing'[5].

[3] https://www.aepd.es/es/documento/guia-rgpd-para-responsables-de-tratamiento.pdf-0
[4] https://www.aepd.es/es/documento/guia-directrices-contratos.pdf
[5] https://www.aepd.es/es/documento/guia-cloud-prestadores.pdf

De esta última se puede extraer un fragmento de su página 5 que ilustra de manera muy sencilla las posiciones y estatus de ambas figuras:

> *«La aplicación de la normativa de protección de datos a la oferta de servicio de cloud computing ha de tener como punto de partida la identificación de la posición jurídica que ocupan, respectivamente, el proveedor de dichos servicios y los clientes con los que contrata.*
>
> *La citada normativa distingue dos sujetos distintos: el responsable del fichero o del tratamiento de los datos y el encargado del tratamiento.*
>
> *El primero es la persona, profesional o entidad que decide sobre la finalidad, contenido y uso del tratamiento.*
>
> *En consecuencia, el cliente que contrata servicios de cloud computing, al tomar decisiones sobre la contratación de dichos servicios, el mantenimiento o no de sus propios sistemas de información, la modalidad de nube y la tipología de servicios que contrata y la elección del proveedor en función de las condiciones ofrecidas, sigue manteniendo la condición de responsable del tratamiento de los datos sobre los que se aplicarán los citados servicios. Esta responsabilidad, al derivarse de la aplicación de la ley, no puede alterarse contractualmente.*
>
> *Por su parte, el proveedor de servicios de cloud computing que implican el acceso a datos personales, aunque sea una gran corporación que se encuentra en una posición prevalente sobre sus clientes, será un prestador de servicios, es decir, un encargado del tratamiento en la terminología de la citada normativa.*
>
> *Esta aproximación inicial sobre la posición jurídica que ocupan el cliente y el prestador de servicios tiene como consecuencia principal la determinación de la ley aplicable, que será la del cliente.»*

Como se puede observar, el tratamiento por medio de un encargado se regirá por un contrato, convenio u otro instrumento jurídico. Dicho instrumento jurídico vinculará al encargado con el responsable y fijará el objeto y la duración del tratamiento, su naturaleza y finalidad, el tipo de datos personales y categorías de interesados, así como sus respectivas obligaciones y derechos. En particular, este instrumento estipulará, entre otras cuestiones, que el encargado actúa únicamente siguiendo las instrucciones del responsable del tratamiento, al cual debe prestar la debida asistencia y con el que debe colaborar para garantizar el cumplimiento de la normativa de protección de datos y los derechos de los interesados. Si un encargado del tratamiento determinase los fines y medios de dicho tratamiento, infringiendo la Ley Orgánica, será considerado responsable con respecto a ese tratamiento. En lo no previsto el encargado del tratamiento se regirá por lo establecido en la Ley Orgánica 3/2018.

Cada responsable debe conservar un registro de todas las actividades de tratamiento de datos personales efectuadas bajo su responsabilidad y, a su vez, cada encargado del tratamiento llevará un registro de todas las actividades de tratamiento de datos personales efectuadas en nombre de un responsable. Tanto uno como otro, llevarán igualmente un registro de operaciones de tratamiento en sistemas de tratamiento automatizados. Ambos tipos de registros estarán a disposición de la autoridad de protección de datos competente a solicitud de esta, y tanto el responsable como el encargado del tratamiento cooperarán con la autori-

dad de protección de datos, en el marco de la legislación vigente, cuando esta lo solicite en el desempeño de sus funciones.

6. Protección de datos desde el diseño y por defecto

Aunque esta es una idea básica que ha venido a implantarse en la normativa aplicable, tampoco es una cuestión que haya aparecido sin más. Ya en la década de los 70[6], la Universidad de Harvard desarrolló un lenguaje de privacidad de alto nivel y un preprocesador para sistemas informáticos que permitía al operador del sistema de datos modificar cualquier programa escrito en un lenguaje convencional (como Cobol). Para ello, profesores como Robert Golberg, propugnaron planes que pretendían separar los aspectos de privacidad de un programa de computadora de sus aspectos funcionales para permitir que el operador del sistema cambiase y modificase el módulo de privacidad a medida que se desarrollase la normativa, sin siquiera tocar el código funcional. Golberg exponía que la codificación de privacidad eficiente permitiría que el sistema se adaptase a las alteraciones y correcciones que pidiese un interesado bajo la entonces Ley Federal de Privacidad, en lugar de simplemente marcar los registros computarizados para que se consultase un archivo manual en busca de registros alterados. O lo que es lo mismo, diseñar un sistema desde la privacidad.

En este campo, correspondiendo con su consideración como principio general de tratamiento y conforme al artículo 28 de la LOPDP, con el objetivo de salvaguardar los principios de protección de datos de forma efectiva e integrar las garantías necesarias en el tratamiento, en el momento de determinar los medios para el tratamiento, así como en el momento del tratamiento propiamente dicho, éste establece que deberán aplicarse las medidas técnicas y organizativas que resulten apropiadas conforme al estado de la técnica y el coste de la aplicación, la naturaleza, el ámbito, el contexto, los fines del tratamiento y los riesgos para los derechos y libertades de las personas físicas desde las fases más tempranas del tratamiento.

Por lo que, antes de dar comienzo al desarrollo de nuevos tratamientos de datos personales, resulta obligatorio pensar en todos los aspectos a tener en cuenta por el responsable y, siempre que se pueda, contar con el parecer del Delegado de Protección de Datos, el cual acompañará y asesorará al responsable de tratamiento antes, durante y después de finalizar estos trabajos.

Entre estas medidas técnicas que se pueden adoptar a los efectos de contribuir a la aplicación de los principios establecidos en esta Ley Orgánica, en especial, el de minimización de datos personales, hay que hacer mención particular a la seudonimización de los datos personales, concepto que, resumidamente, implica que el tratamiento de los mismos se realice de manera tal que no puedan atribuirse a un interesado sin utilizar información adicional.

Además, las medidas técnicas y organizativas deben garantizar que, por defecto, sólo sean objeto de tratamiento los datos personales que resulten estrictamente necesarios para cada uno de los fines específicos del tratamiento y que las medidas de seguridad más elevadas de protección sean las que se dispongan en la primera configuración para las actividades a llevar a cabo. Dicha obligación se

[6] GOLBERG.R. Privacy Journal, nº 12 October 1975. P.O. BOX 8844.

aplicará tanto a la cantidad de datos personales recogidos, como a la extensión de su tratamiento, a su período de conservación y a su accesibilidad. Tales medidas tienen por objeto garantizar que, por defecto y entre otras cuestiones, los datos personales no sean accesibles a un número indeterminado de personas sin intervención humana.

7. Registro de Actividades de Tratamiento (RAT) y Registro de Operaciones (ROP)

El RAT se encuentra previsto en el artículo 32 de la norma. De acuerdo con el contenido de este precepto, cada responsable de tratamiento debe conservar un registro de todas las actividades de tratamiento de datos personales efectuadas bajo su responsabilidad. Dicho registro deberá contener la información siguiente:

- La identificación del responsable del tratamiento y sus datos de contacto, así como, en su caso, del corresponsable y del delegado de protección de datos.
- Los fines del tratamiento.
- Las categorías de destinatarios a quienes se hayan comunicado o vayan a comunicarse los datos personales, incluidos los destinatarios en Estados que no sean miembros de la Unión Europea u organizaciones internacionales.
- La descripción de las categorías de interesados y de las categorías de datos personales.
- El recurso a la elaboración de perfiles, en su caso.
- Las categorías de transferencias de datos personales a un Estado que no sea miembro de la Unión Europea o a una organización internacional, en su caso.
- La indicación de la base jurídica del tratamiento, así como, en su caso, las transferencias internacionales de las que van a ser objeto los datos personales.
- Los plazos previstos para la supresión de las diferentes categorías de datos personales, cuando sea posible.
- La descripción general de las medidas técnicas y organizativas de seguridad a las que se refiere el artículo 37.1 de la Ley, cuando sea posible.

Por su parte, cada encargado del tratamiento llevará un registro de todas las actividades de tratamiento de datos personales efectuadas en nombre de un responsable. Este registro contendrá la información siguiente:

- El nombre y los datos de contacto del encargado o encargados del tratamiento, de cada responsable del tratamiento en cuyo nombre actúe el encargado y, en su caso, del delegado de protección de datos.
- Las categorías de tratamientos efectuados en nombre de cada responsable.
- Las transferencias de datos personales a un Estado que no sea miembro de la Unión Europea o a una organización internacional, en su caso, incluida la identificación de dicho Estado o de dicha organización internacional cuando el responsable del tratamiento así lo ordene explícitamente.
- La descripción general de las medidas técnicas y organizativas de seguridad a las que se refiere el artículo 37.1 de esta Ley, cuando sea posible.

Los Registros de Actividades de Tratamiento se establecerán y llevarán por escrito, admitiéndose la posibilidad del formato electrónico, y estarán a disposición de la autoridad de protección de datos competente, a solicitud de esta, de conformidad con lo dispuesto legalmente. Los responsables de los tratamientos harán público el registro de sus actividades de tratamiento, que deberá ser accesible por medios electrónicos.

El contenido del RAT del Ministerio del Interior figura publicado tanto en la página web del Departamento como en la página del Portal de Transparencia.

Por su parte, el ROP constituye una de las novedades relativas al ámbito de los tratamientos de datos realizados con finalidad policial y sería una de las bases instrumentales del sistema de autorregulación de los responsables. Se trata de un sistema de control obligatorio impuesto por el artículo 25 de la DDP y recogido a su vez en el artículo 33 de la LOPDP, conforme al cual los responsables y encargados de tratamiento deben mantener registros que recojan la identificación, autenticación y trazabilidad en los sistemas automatizados de, al menos, las operaciones de siguientes:

- Recogida.
- Alteración.
- Consulta.
- Comunicación incluidas las posibles transferencias.
- Combinación.
- Supresión.

Dentro de estos, los registros de «consulta» y «comunicación» harán posible determinar:

- La justificación.
- La fecha y la hora de tales operaciones.
- En la medida de lo posible, el nombre de la persona que consultó o comunicó datos personales, así como la identidad de los destinatarios de dichos datos personales.

Éstos se utilizarán únicamente a efectos de verificar la legalidad del tratamiento, autocontrol, garantizar la integridad y la seguridad de los datos personales y en el ámbito de los procesos penales y serán puestos a disposición de la autoridad de control competente, previa solicitud de esta, y siempre conforme a la legalidad vigente.

Es asimismo muy importante incorporar esta herramienta obligatoria como elemento de responsabilidad proactiva y control del acceso o cesiones no autorizadas a los tratamientos. Aunque posteriormente se estudiará con más profundidad las distintas y posibles responsabilidades en la materia, resultaría relevante conocer el contenido de las siguientes sentencias del Tribunal Supremo relacionadas con esta obligación: STS 743/2021 - ECLI:ES:TS:2021:743, STS 832/2021 - ECLI:ES:TS:2021:832 y STS 1153/2021 - ECLI:ES:TS:2021:1153, al objeto de valorar, por parte de las autoridades competentes, la autenticación y la trazabilidad en todos los accesos, cesiones o traslados de datos personales de los que sean responsables.

CAPÍTULO 3
DERECHOS DE LOS INTERESADOS

I. REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS

1. Introducción

La protección efectiva de los datos personales en la Unión Europea exige que se refuercen y especifiquen los derechos de los interesados y las obligaciones de quienes tratan y determinan el tratamiento de los mismos, y que en los Estados miembros se reconozcan poderes equivalentes para supervisar y garantizar el cumplimiento de las normas aplicables y que las infracciones se castiguen con sanciones equivalentes, tal como se reconoce en el considerando 11 del RGPD.

Con anterioridad a la presente estructura de derechos de los interesados, en nuestro país, la LORTAD y posteriormente la LOPD desarrollaron un sistema que se basaba en los famosos derechos ARCO (Acceso, Rectificación, Cancelación y Oposición).

En concreto, en base a la LORTAD, el primer instrumento jurídico que se podría analizar sería la Instrucción 1/1998, de 19 de enero, de la Agencia de Protección de Datos, relativa al ejercicio de los derechos de acceso, rectificación y cancelación[1]. Ésta sería la primera etapa del ejercicio de los derechos por los interesados y como se apuntó estaba basada en el acceso a los ficheros automatizados.

Esta Instrucción señalaba que los derechos eran personalísimos e independientes y dejaba el ejercicio por el afectado frente al responsable del fichero por lo que entendía necesario que el afectado acreditase su identidad frente a dicho responsable y que no podía entenderse que el ejercicio de ninguno de ellos sea requisito previo para el ejercicio de otro.

Posteriormente la LOPD disponía que los interesados ostentaban los derechos ARCO y que los procedimientos para ejercitarlos serían establecidos reglamentariamente. Siendo una primera condición la exigencia de no solicitar alguna compensación por el ejercicio de los derechos.

---

[1] Agencia de Protección de Datos. «BOE» núm. 25, de 29 de enero de 1998. Referencia: BOE-A-1998-1943

El RLOP si desarrolló un título concreto, el III, para establecer el procedimiento completo para el ejercicio de los derechos de los interesados (Vid. Artículos 23 a 36)

En la actualidad, el legislador europeo vino a establecer la existencia del deber de transparencia del responsable, el cual lleva aparejado necesariamente el derecho de los interesados a ser a ser informados por aquellos sobre cualquier tratamiento que lleven a cabo con sus datos, si bien, este derecho estaría sujeto a diferentes restricciones, excepciones o limitaciones.

De hecho, en el considerando 58, de manera que inspire la parte dispositiva del instrumento normativo, se viene a declarar que:

> *«El principio de transparencia exige que toda información dirigida al público o al interesado sea concisa, fácilmente accesible y fácil de entender, y que se utilice un lenguaje claro y sencillo, y, además, en su caso, se visualice. Esta información podría facilitarse en forma electrónica, por ejemplo, cuando esté dirigida al público, mediante un sitio web. Ello es especialmente pertinente en situaciones en las que la proliferación de agentes y la complejidad tecnológica de la práctica hagan que sea difícil para el interesado saber y comprender si se están recogiendo, por quién y con qué finalidad, datos personales que le conciernen, como es en el caso de la publicidad en línea. Dado que los niños merecen una protección específica, cualquier información y comunicación cuyo tratamiento les afecte debe facilitarse en un lenguaje claro y sencillo que sea fácil de entender».*

Es un elemento esencial del RGPD que se facilite el ejercicio de estos derechos, de manera que se proporcionen mecanismos para solicitar y, en su caso, obtener de forma gratuita, en particular, el acceso a los datos personales y su rectificación o supresión, así como el ejercicio de los derechos de oposición, limitación portabilidad de los datos a través de sistemas interoperables y a no ser sometido decisiones automatizadas perjudiciales.

Un supuesto que se refuerza es el *«derecho al olvido»* como una parte del derecho de supresión en el entorno en línea de manera que se impida la difusión de información personal a través de Internet cuando su publicación no cumpla los requisitos de adecuación y pertinencia previstos en la normativa. En concreto, incluye el derecho a limitar la difusión universal e indiscriminada de datos personales en los buscadores generales cuando la información es obsoleta o ya no tiene relevancia ni interés público, aunque la publicación original fuese legítima.

El Convenio 108+[2] enumera otra serie de derechos específicos, como sería el derecho a obtener, previa solicitud, la información sobre el razonamiento subyacente al tratamiento de los datos cuando los resultados de los datos les sean aplicables a los interesados, del mismo modo fija la necesidad de tener reconocido por las legislaciones nacionales un recurso cuando los derechos incluidos en dicho Convenio hayan sido vulnerados y el derecho a beneficiarse de la asistencia de una autoridad de control el ejercicio de estos derechos con independencia de su nacionalidad o residencia.

[2] https://www.coe.int/es/web/data-protection/convention108-and-protocol

Ante un breve o somero análisis de las relaciones que llevamos a cabo y que derivan en el tratamiento de nuestros datos, se puede observar la clara desigualdad entre las relaciones entre los responsables del tratamiento y los interesados, que con este marco legal se ve atenuada precisamente por los derechos específicos reconocidos a éstos de manera que se les permite tener un mayor y mejor control sobre los mismos.

En este aspecto se habría de tener en consideración la siguiente cuestión: *la eficacia de estos derechos vendrá delimitada en gran parte por la existencia de mecanismos adecuados para poder ejercerlos apropiadamente.*

En nuestro país, con el fin de adaptar nuestro ordenamiento jurídico al RGPD, se aprobó la LOPDGDD. Por ello, en el presente Capítulo se estudiarán las previsiones contenidas en una y otra norma al objeto de dotar de habitualidad el manejo de ambas.

Debe tenerse presente, en cualquier caso, tal y como se viene detallando, que existe un régimen específico en el *«ámbito policial»*, regulado en la DDP que se ha transpuesto en nuestro ordenamiento mediante la LOPDP.

En este capítulo se estudiarán pormenorizadamente los derechos de las personas contenidos en los citados instrumentos normativos, así como otras cuestiones relacionadas que resultan igualmente relevantes.

Con el fin de llevarlo a cabo de una manera sencilla y clara, se distinguen separadamente los principales derechos previstos, primero con carácter general, para luego establecer las especificidades que afectan a los miembros de las Fuerzas y Cuerpos de Seguridad en funciones de detección, prevención e investigación delictiva. Por último, se agrupan en un epígrafe unas cuestiones relevantes relacionadas con el ejercicio de los derechos, tales como los supuestos de detección de las llamadas brechas de seguridad, se estudia la regulación de los derechos digitales, y se señalan las previsiones más importantes del Protocolo General de Actuación entre el Ministerio del Interior y la Agencia Española de Protección de Datos en materia de atención a las personas afectadas en caso de que sus datos se hayan obtenido ilegítimamente y difundido a través de internet.

Veamos a continuación con detalle los aspectos relativos a los derechos de las personas, regulados en el Capítulo III del RGPD, artículos 12 a 23. Asimismo, se reflejan los contenidos de la Guía para el cumplimiento del deber de informar elaborada por la Agencia Española de Protección de Datos.

2. Transparencia e información. Características generales

2.1. Transparencia

En virtud del principio de transparencia (artículo 12 RGPD) se desprenden unas obligaciones concretas en relación con el deber de informar por parte del responsable del tratamiento, de tal forma que debe ser:

- Concisa, lo cual, según la RAE exige *«Brevedad y economía de medios en el modo de expresar un concepto con exactitud.»*
- Transparente, cuya acepción oportuna en la RAE sería que la información resulta: «Claro, evidente, que se comprende sin duda ni ambigüedad»

- Inteligible, de manera que la información pueda ser entendida por cada una de las personas a las que va dirigida.
- De fácil acceso, a través de sistemas o canales que no impongan dificultades para su ejercicio y utilizando un lenguaje claro y sencillo adaptado a los destinatarios.
- Por escrito o por otros medios, incluso electrónicos.

2.2. Derecho de Información

El responsable del tratamiento, en base a ese deber de ser transparente facilitará al afectado/interesado la siguiente información:

- Básica (como mínimo). A continuación, se detallará el contenido de esta información básica, en función de si los datos se obtienen o no del interesado.
- Adicional: Dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata a la restante información.

Debe tenerse en cuenta al respecto que:
Cuando los datos personales se obtengan del interesado se informará de:

- Identidad y datos de contacto del responsable y en su caso de su representante.
- Finalidad del tratamiento y base jurídica del tratamiento.
- Plazo de conservación de los datos personales.
- Existencia del derecho a solicitar al responsable de tratamiento el acceso, rectificación, supresión, limitación de su tratamiento, oposición o la portabilidad de los datos personales relativos al interesado.
- Posibilidad de revocar el consentimiento prestado
- Derecho a presentar una reclamación ante la autoridad de control (AEPD).

Además, en su caso, se deberá facilitar al interesado:

- Datos de contacto del DPD
- Interés legítimo del responsable o un tercero
- Destinatarios o categorías
- Intención del responsable de transferir datos personales a un tercer país u organización internacional
- Existencia de decisiones individualizadas automatizadas, incluida la elaboración de perfiles
- Existencia de comunicaciones de datos, por requisito legal o contractual, y de la obligación a facilitar dichos datos, consecuencias de la negativa a facilitarlos.

Cuando los datos no hayan sido recabados del interesado, el responsable deberá facilitar, además de la información anterior:

- El origen de los datos
- La categoría de los datos.

2.3. Aspectos a tener en cuenta respecto a la información de los derechos

Momento en el que se ha de informar al interesado

Si se recaban directamente del interesado: en el momento en que se soliciten, previo a la recogida o registro.

Si no se obtienen del propio interesado:

- Antes de un mes desde que se obtuvieron los datos
- A más tardar en el momento de la primera comunicación con el interesado, si los datos personales han de utilizarse para comunicación con el interesado.
- Antes de que los datos personales se hayan comunicado por primera vez, en caso de estar previsto que sean comunicados a otro destinatario.

No obstante, el artículo 14.5 del RGPD prevé que no es preciso informar a la persona interesada cuando sus datos no se hayan obtenido de la misma, cuando:

- El interesado ya disponga de la información puesto que el responsable del tratamiento que los obtiene de manera directa haya informado cumplida y totalmente del tratamiento a llevar a cabo con sus datos.
- La comunicación de dicha información resulte imposible o suponga un esfuerzo desproporcionado, en particular para el tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, a reserva de las condiciones y garantías indicadas en el artículo 89, apartado 1, o en la medida en que la obligación mencionada en el apartado 1 del presente artículo pueda imposibilitar u obstaculizar gravemente el logro de los objetivos de tal tratamiento. En tales casos, el responsable adoptará medidas adecuadas para proteger los derechos, libertades e intereses legítimos del interesado, inclusive haciendo pública la información.
- La obtención o la comunicación esté expresamente establecida por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca medidas adecuadas para proteger los intereses legítimos del interesado.

  Esta cuestión resulta muy interesante puesto que el deber de informar no decae por parte del interesado que trata los datos directamente del interesado, sino que puede no ser necesario que se traslade la información por parte del organismo que recibe dichos datos por obligación legal. Veamos un ejemplo: Si un establecimiento de hospedajes trata datos con la finalidad de cumplir con la obligación de registro documental e información derivada del artículo 25.1 de la LOPSC, entendemos que los recoge directamente de la persona interesada por obligación legal y por lo tanto debería facilitarle la información oportuna sobre el tratamiento a llevar cabo, si bien, esa obligación de información no se extendería al organismo competente al que se comunica dicha información; en este caso al Ministerio del Interior.
- Cuando los datos personales deban seguir teniendo carácter confidencial sobre la base de una obligación de secreto profesional regulada por el

Derecho de la Unión o de los Estados miembros, incluida una obligación de secreto de naturaleza estatutaria. Cuestión ésta que es de directa aplicación a la información y los datos que traten los miembros de las Fuerzas y Cuerpos de Seguridad en los distintos procedimientos a llevar a cabo en cumplimiento de sus misiones al verse éstos sometidos estatutariamente a guardar riguroso secreto de todas las informaciones que conozcan por razón de su cargo o con ocasión del desempeño de sus funciones en cumplimiento del artículo 5.5 de las LOFSC.

¿Cómo informar a los interesados?

No hay establecido un único modo para ello, sino que la información a facilitar debe adaptarse a las circunstancias de cada uno de los medios empleados para el registro de los datos. De tal manera, puede informase a través de:

- Formularios en papel-entrevista telefónica
- Navegación o formularios web
- Registro de aplicaciones móviles
- Datos de actividad personal
- Datos de sensores

Las comunicaciones al interesado sobre datos ya disponibles o tratamientos adicionales pueden hacerse llegar por correo postal, mensajería electrónica o notificaciones emergentes en servicios o aplicaciones.

Información por capas derivada del contenido de *la «Guía para el cumplimiento del deber de informar»* de la AEPD, la Agencia Vasca de Protección de Datos y la Autoridad Catalana de Protección de Datos.[3].

Epígrafe	Información básica (1ª capa, resumida)	Información adicional (2ª capa, detallada)
«Responsable» (del tratamiento)	Identidad del Responsable del tratamiento	Datos de contacto del Responsable
		Identidad y datos de contacto del representante
		Datos de contacto del Delegado de Protección de Datos
«Finalidad» (del tratamiento)	Descripción sencilla de los fines del tratamiento, incluso elaboración de perfiles	Descripción ampliada de los fines del tratamiento
		Plazos o criterios de conservación de los datos
		Decisiones automatizadas, perfiles y lógica aplicada

[3] https://www.aepd.es/sites/default/files/2019-11/guia-modelo-clausula-informativa.pdf

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

La LOPDGDD habla de contenido mínimo, sin embargo, la AEPD en su *«Guía para el cumplimiento del deber de informar»*[4], establece una división en dos capas. A saber:

Primer nivel: supone presentar una información básica de forma resumida, en el mismo momento y en el mismo medio en que se recojan los datos.

Segundo nivel: donde se presentan detalladamente el resto de informaciones, en un medio más adecuado para su presentación, comprensión y archivo.

A modo de ejemplo, la AEPD ha propuesto un cuadro en el que se muestra la información en las dos capas diferentes en función del tipo de datos a ofrecer, *Responsable; Finalidad; Legitimación; Destinatarios; Derechos; Procedencia de los datos.*

[4] https://www.aepd.es/sites/default/files/2019-11/guia-modelo-clausula-informativa.pdf

2.4. Características generales comunes

El considerando 59 RGPD anticipa las líneas generales de la protección dispensada a los derechos de los ciudadanos al señalar que:

> *«Deben arbitrarse fórmulas para facilitar al interesado el ejercicio de sus derechos en virtud del presente Reglamento, incluidos los mecanismos para solicitar y, en su caso, obtener de forma gratuita, en particular, el acceso a los datos personales y su rectificación o supresión, así como el ejercicio del derecho de oposición. El responsable del tratamiento también debe proporcionar medios para que las solicitudes se presenten por medios electrónicos, en particular cuando los datos personales se tratan por medios electrónicos. El responsable del tratamiento debe estar obligado a responder a las solicitudes del interesado sin dilación indebida y a más tardar en el plazo de un mes, y a explicar sus motivos en caso de que no fuera a atenderlas».*

En este punto, podemos destacar de manera esquemática las siguientes características respecto al ejercicio de los derechos:

- Personalísimo: la solicitud solo puede ser presentada por el propio afectado, representante legal (incapaz o menor de edad) o representante voluntario designado expresamente por el afectado.
- Cuando el responsable tenga dudas sobre la identidad del solicitante, el responsable solicitará fotocopia del DNI o documento equivalente que acredite la identidad y sea válido en derecho.
- En caso de que se actúe a través de representación legal deberá aportarse, además, DNI y documento acreditativo de la representación del representante.
- No formalidad: hay que atender la solicitud, aunque el solicitante no haya usado el procedimiento establecido, siempre que pueda acreditar el envío y recepción.
- Independencia: el ejercicio de ninguno de ellos es requisito previo para el ejercicio de otro.
- Sencillez y gratuidad: la información debe proporcionarse en forma inteligible y de fácil acceso, con un lenguaje claro, utilizando un medio sencillo y gratuito para el ejercicio de los derechos.
- No obstante, cuando las solicitudes sean manifiestamente infundadas o excesivas, el responsable podrá cobrar un canon razonable o negarse a actuar. En este caso, la carga de la prueba: corresponde al responsable, debiendo conservar la acreditación del cumplimiento del mencionado deber.
- Plazo de 1 mes: para atender las solicitudes de ejercicio de cualquiera de los derechos. Podrá extenderse 2 meses más cuando se trate de solicitudes especialmente complejas. El responsable deberá notificar esta ampliación dentro del primer mes.
- Si el responsable decide no atender una solicitud, deberá informar de ello, motivando su negativa, dentro del plazo de 1 mes desde su presentación e informará de la posibilidad de presentar una reclamación ante las autoridades de control.

- Colaboración del encargado de tratamiento: el responsable podrá contar con la colaboración del encargado para el ejercicio de los derechos, pudiendo incluirla en el contrato de encargado de tratamiento.

2.5. Cuestiones procedimentales referentes al ejercicio y atención de los derechos

La solicitud de ejercicio de los derechos podría detallarse de la siguiente forma:

¿A quién se dirige?

Se dirigirá al responsable del tratamiento o al delegado de protección de datos.

Cuando existan dos o más corresponsables de tratamiento, indistintamente frente a cada uno de los responsables (significar que éstos pueden acordar otro procedimiento puesto que pueden articular un sistema procedimental propio).

Cuando se ejerciten ante el encargado de tratamiento, éste dará traslado al responsable, salvo que en el contrato se establezca que lo atiende el propio encargado.

Contenido de la solicitud

- Nombre y apellidos del interesado y documento que acredite la personalidad o representación.
- Petición en que se concreta la solicitud.
- Dirección a efectos de notificaciones, fecha y firma del solicitante.
- Documentos acreditativos de la petición que formula, en su caso. En la solicitud del derecho de rectificación, y en el supuesto de datos incompletos, el interesado entregará una declaración adicional con el fin de completar los datos.

2.6. La respuesta al interesado

¿Cuándo se atiende la solicitud?

En relación con la atención de la solicitud deben tenerse en cuenta las siguientes circunstancias:

Plazo: sin demora y en el plazo máximo de un mes.

Prórroga: podrá prorrogarse por otros dos meses en caso necesario, teniendo en cuenta la complejidad de la solicitud y el número de solicitudes. Deberá informarse el interesado del motivo del retraso dentro de un mes a contar desde la recepción de la solicitud.

Subsanación: en caso de que la solicitud no contemple la información requerida, el responsable deberá solicitar la subsanación de la misma (en este caso se suspenden los plazos).

No atención: si el responsable del tratamiento no da curso a la solicitud del interesado, le informará sin demora injustificada, y a más tardar al mes de la recepción de la solicitud, de las razones por las que no ha actuado, así como de la posibilidad de presentar una reclamación ante una autoridad de control y recurrir a los tribunales.

Actuación del responsable de tratamiento

El responsable deberá:

- Atender las solicitudes enviadas por las personas cuyos datos se encuentran en los ficheros de datos de carácter personal que dispone, respondiendo en los términos establecidos en la normativa.
- Facilitar a los interesados el ejercicio de sus derechos, procurando que los procedimientos y las formas que se faciliten a los interesados para el ejercicio de sus derechos sean visibles, accesibles y sencillos.
- Solicitar al afectado o interesado la enmienda de los derechos que puedan tener las solicitudes que no reúnan los requisitos que exigen las normas.

Actuación del responsable de seguridad o DPO

- Control y revisión del trámite de la solicitud del interesado
- Proceder al alta de las solicitudes en el registro que se haya constituido al efecto.
- Dar respuesta a la solicitud del interesado.

3. Derecho de acceso

Es el derecho del interesado a obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que le conciernan. Forma parte del derecho a la intimidad.

Dentro de la legislación de la U.E. podemos citar con carácter general el contenido de los artículos 8.2 de la Carta, 15 del RGPD o 15 de la DDP. Sin dejar de mencionar, que en el artículo 9.1 del Convenio 108+ también se detalla pormenorizadamente dicho presupuesto y que ése figura en varias recomendaciones del Consejo de Europa[5].

Según tiene declarado el TEDH[6] se debe entender que existe un derecho de acceso a la información sobre los datos de las personas interesadas que sean tratados por terceros y que este derecho se deriva de la necesidad de proteger la vida privada; asimismo, el Tribunal Constitucional, el derecho de acceso se articula como eje fundamental para el ejercicio de los derechos del interesado. Conocer quién posee los datos personales y controlar su uso y fin al que se destina esa

[5] https://www.coe.int/en/web/data-protection/legal-instruments

[6] Asunto: 10454/83 GASKIN Vs. The United Kingdom https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-57491%22]}

información es garantía indispensable en una efectiva protección de la esfera privada constitucionalmente protegida. Por ello, se ha venido en considerar como paso previo para el ejercicio de otros derechos.

Este derecho de acceso comprende que se facilite a la persona interesada, al menos, la siguiente información:

- Fines del tratamiento.
- Categorías de datos personales de que se trate.
- Destinatarios o categorías de destinatarios a los que se comunicarán los datos.
- Plazo durante el cual se conservarán los datos personales o, cuando eso no sea posible, los criterios utilizados para determinar este plazo.
- Existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, y a oponerse al tratamiento.
- El derecho a presentar una reclamación ante una autoridad de control.
- La fuente de la que proceden los datos personales y, en su caso, si proceden de fuentes de acceso público.
- La existencia de decisiones automatizadas, incluida la elaboración de perfiles, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.
- Cuando se transfieran datos personales a un tercer país o a una organización internacional, el interesado tendrá derecho a ser informado de las garantías adecuadas.

Si el responsable trata una gran cantidad de datos, podrá solicitar al interesado que especifique los datos o actividades de tratamiento a los que se refiere en la solicitud si no aclara si se refiere a todos o a una parte de ellos.

Este derecho se entenderá realmente facilitado si el responsable proporcionara al afectado un sistema de acceso remoto, directo y seguro a los datos personales que garantice, de modo permanente, el acceso a su totalidad. A tales efectos, la comunicación por el responsable al afectado del modo en que se podrá acceder a dicho sistema bastará para tener por atendida la solicitud de ejercicio del derecho.

Esta copia se proporcionará a través de alguna de las formas siguientes:

- Visualización en pantalla.
- Por escrito, copia o fotocopia remitida por correo, certificado o no.
- Correo electrónico u otros sistemas de comunicaciones electrónicas.
- Facilitando el acceso remoto a un sistema seguro que ofrezca al interesado un acceso directo a sus datos personales.

El responsable deberá facilitar una copia de los datos objeto de tratamiento. Si el interesado solicita otra copia, podrá ser remunerada con una tasa o canon razonable. La LOPDGDD considera repetitivo el ejercicio de derecho de acceso cuando se solicite en más de una ocasión durante el plazo de seis meses, a menos que exista causa legítima. Por otro lado, la solicitud se considerará excesiva, asu-

miendo el interesado el exceso de costes que comporte, cuando el interesado eligiese un medio distinto al ofrecido por el responsable.

En este contexto es ineludible señalar, tal y como se recoge en el expediente nº TD/00140/2021 de la AEPD, que no entran dentro del derecho de acceso las valoraciones subjetivas que pueda hacer un profesional ni la copia de documentos.

Cuestión ésta que tambien está recogida en las Recomendaciones 1/2022, sobre el derecho de acceso del Comité Europeo de Protección de Datos (publicadas para consulta pública[7]) donde, entre otras muchas cuestiones, se reincide sobre la idea de que la obligación de facilitar copia se refiere, únicamente, a datos personales y no a los documentos originales que los contienen.

El derecho de acceso es independiente del derecho de acceso a la información pública que regula la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno. También es independiente del derecho de acceso a la documentación en un procedimiento administrativo, regulado por la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

Por su parte, el acceso a la historia clínica se regula específicamente en la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica –«Ley de Autonomía del Paciente», si bien la autoridad competente en materia de protección de datos podrá tutelar este acceso en caso de que -una vez ejercitado- la respuesta no sea satisfactoria para el ciudadano, o no se haya respondido en los plazos previstos. Además, esta Ley permite el acceso a la historia clínica de los pacientes fallecidos a personas vinculadas con él, por razones familiares o de hecho, salvo que el fallecido lo hubiese prohibido expresamente y así se acredite.

4. Derecho de rectificación

El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la rectificación de los datos personales inexactos que le conciernan.

Teniendo en cuenta los fines del tratamiento, igualmente tendrá derecho a que se completen los datos personales que sean incompletos, inclusive mediante una declaración adicional.

Esta posibilidad es una consecuencia lógica del ejercicio del derecho de acceso.

La expresión sin dilación indebida hay que conjugarla con el plazo general de un mes y en su caso la posibilidad de prórroga (dos meses en función de la complejidad y el número de solicitudes).

Al ejercer este derecho el afectado deberá indicar en su solicitud a qué datos se refiere y la corrección que haya de realizarse, acompañando la documentación justificativa de la inexactitud o carácter incompleto de los datos, cuando ello sea preciso.

[7] https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-012022-data-subject-rights-right_es

Por ejemplo, cuando el titular de los datos cambia de domicilio y la dirección que posee la Administración pública -responsable del tratamiento-, es la anterior, a través del ejercicio de este derecho dicho titular puede comunicar la nueva dirección, instando la rectificación de sus anteriores datos personales.

Bloqueo:

Según lo establecido en el artículo 32 de la LOPDGDD

El responsable está obligado a bloquear los datos cuando proceda a su rectificación o supresión.

Los datos bloqueados quedarán a disposición exclusiva de los jueces y tribunales, el Ministerio Fiscal o las Administraciones públicas competentes, para la exigencia de posibles responsabilidades derivadas del tratamiento y por el plazo de prescripción de las mismas. Transcurrido ese plazo, deberá procederse a la destrucción de los datos.

Cuando para el cumplimiento de esa obligación, la configuración del sistema de información no permita el bloqueo o se requiera una adaptación que implique un esfuerzo desproporcionado, se procederá a un copiado seguro de la información de modo que conste evidencia digital, o de otra naturaleza, que permita acreditar la autenticidad de la misma, la fecha del bloqueo y la no manipulación de los datos durante el mismo.

Excepciones:

- Tratamiento de videovigilancia.
- Sistemas de información de denuncias internas en el sector privado *(whistleblowers o alertadores, figura que próximamente se regulará al transponer la Directiva (UE) 2019/1937 del Parlamento Europeo y del Consejo, de 23 de octubre de 2019, relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión*).

5. Derecho de supresión (el derecho al olvido)

Tradicionalmente era conocido como derecho de cancelación.

El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión-eliminación de los datos personales que le conciernan del fichero de tratamiento, cuando concurra alguna de las circunstancias siguientes:

- Datos innecesarios
  Cuando los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo.

- Sin consentimiento
  Cuando el interesado retire el consentimiento en que se basa el tratamiento y este no se base en otro fundamento jurídico.

- Oposición
  Cuando el interesado se oponga al tratamiento y no prevalezcan otros motivos legítimos para el tratamiento.

- Ilicitud
  Cuando los datos personales hayan sido tratados ilícitamente.

- Obligación legal
  Cuando los datos personales deben 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.

- Menores
  Cuando los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información dirigidos a menores.

Este derecho es una manifestación de los derechos de cancelación u oposición en el entorno online. Hace referencia al derecho a impedir la difusión de información personal a través de internet cuando su publicación no cumple los requisitos de adecuación y pertinencia previstos en la normativa. En concreto, incluye el derecho a limitar la difusión universal e indiscriminada de datos personales en los buscadores generales cuando la información es obsoleta o ya no tiene relevancia ni interés público, aunque la publicación original sea legítima.

No es necesario que el interesado sufra un perjuicio para que ejerza el derecho al olvido.

Los ejemplos más típicos se vinculan al tratamiento ilícito de datos, o a la desaparición de la finalidad que motivó el tratamiento para el que fueron recogidos.

En estos casos, sería interesante la implementación de medidas procedimentales que reforzaran la responsabilidad proactiva como el desarrollar un sistema de certificados

No obstante, no procederá la supresión cuando sea necesario para:

- Ejercer el derecho a la libertad de expresión e información.
- El cumplimiento de una obligación legal que requiera el tratamiento de datos impuesta por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento.
- Para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable.
- Por razones de interés público en el ámbito de la salud pública.
- Con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, en la medida en que el derecho indicado en el apartado 1 pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento, o.
- La formulación, el ejercicio o la defensa de reclamaciones.
- El responsable podrá conservar los datos identificativos del afectado necesarios con el fin de impedir tratamientos futuros para fines de mercadotecnia directa.

Deben destacarse en este epígrafe los dos nuevos derechos introducidos en el Título X de la LOPDGDD: derecho al olvido en las búsquedas de internet (art. 93) y derecho al olvido en servicios de redes sociales y servicios equivalentes (art. 94).

Podemos resumirlo en los siguientes puntos:

- Supone aplicar los derechos de cancelación y oposición a los buscadores para impedir la difusión de la información cuando ésta es obsoleta o no tiene relevancia ni interés público.
- Si se estima tu pretensión, la información no aparecerá en los resultados de búsquedas, pero seguirá publicado en la fuente original.
- Se debe valorar caso a caso para lograr un equilibrio entre los diferentes derechos e intereses afectados.
- Si los buscadores deniegan tu pretensión puedes interponer una reclamación ante la AEPD.
- Los principales buscadores han habilitado formularios para facilitar su ejercicio. Puedes encontrarlos en la sección web de la AEPD sobre el derecho al olvido.
- Puedes ejercitarlo ante los buscadores sin necesidad de acudir a la fuente original de publicación.

Al hilo del estudio de estos derechos, debe destacarse que la AEPD fue pionera al considerar que el tratamiento de datos que realizan los motores de búsqueda de internet, tales como Google, Bing o Yahoo, está sometido a las normas de protección de datos de la Unión Europea, y que los ciudadanos pueden solicitar, bajo ciertas condiciones, que los enlaces a sus datos personales no aparezcan en los resultados de una búsqueda realizada por su nombre y apellidos. Esta tesis propugnada por la AEPD fue avalada en 2014 por el Tribunal de Justicia de la Unión Europea, y se popularizó con la denominación de *«derecho al olvido»*[8].

En esencia, el *«derecho al olvido»* supone lo siguiente:

- La aplicación de los derechos de supresión y oposición a los buscadores de internet para impedir la difusión de la información cuando ésta es obsoleta o no tiene relevancia ni interés público.
- Si se estima la pretensión del interesado, la información no aparecerá en los resultados de búsquedas, pero –salvo que el *«editor»* (fuente original) adopte medidas al respecto- se seguirá publicado en la fuente original.
- El ejercicio de este derecho, y su eventual atención, se deben valorar caso a caso para lograr un equilibrio entre los diferentes derechos e intereses en juego.
- Si los responsables de los buscadores de internet deniegan la pretensión de un interesado, éste puede presentar una reclamación ante la Agencia.
- Los principales buscadores de internet han habilitado formularios para facilitar su ejercicio. También pueden obtenerse dichos formularios y/o enlaces en la sección web de la Agencia dedicada al *«derecho al olvido»*.
- El interesado puede ejercitar este derecho ante los buscadores sin necesidad de acudir a la fuente original de publicación.

[8] Asunto C-131/12, Google Spain, Google Inc. v Agencia Española de Protección de Datos (AEPD)

Por lo que se refiere a la eliminación de fotos y vídeos que hayan sido publicados en internet sin el consentimiento de los interesados, se puede también ejercitar el derecho de supresión.

Para ello el interesado debe dirigirse ante el responsable que haya publicado la información en la red, acreditando su identidad, indicando los enlaces donde aparecen los vídeos y fotos, y solicitando el borrado de los mismos.

Por otra parte, las redes sociales más populares ofrecen servicios de ayuda que permiten poner en su conocimiento, a través de sus propios formularios, cuándo se ha producido una vulneración de la privacidad o se han volcado contenidos inapropiados.

Con la finalidad de facilitar su ejercicio, en la web de la AEPD, en el *«Canal Ciudadano»*, existe un apartado específico referido sobre *«Eliminar vídeos y fotos de Internet»*, con enlaces a los citados servicios de ayuda de las redes sociales más utilizadas.

En relación con este derecho, el reciente Dictamen 39/2021, de Comité Europeo de Protección de Datos sobre si el artículo 58, apartado 2, letra g), del RGPD podría servir de base jurídica para que una autoridad de control ordene de oficio la supresión de datos personales, en caso de que dicha solicitud no haya sido presentada por el interesado[9], ha expuesto que el artículo 17 del RGPD recoge dos elementos fundamentales: la supresión a petición del interesado y la supresión como una obligación del responsable. Esto supondría que los responsables tienen que detectar por si mismos distintas situaciones en las que deben suprimir los datos en aras del principio de responsabilidad activa. Es por ello que las autoridades independientes de control competentes deben asegurar que esto se produce, aunque las personas interesadas no estén informadas, no sean conscientes del tratamiento de sus datos o en los supuestos en los que no todos los interesados hayan ejercido este derecho.

6. Derecho a la limitación del tratamiento

El artículo 4 del RGPD lo define como el marcado de los datos de carácter personal conservados con el fin de limitar su tratamiento en el futuro. Se trata de una medida cautelar que reduce el tratamiento de los datos personales a la conservación.

El interesado tendrá derecho a obtener del responsable del tratamiento la limitación del tratamiento cuando se cumpla alguna de las condiciones siguientes:

- Impugnación- cuando el interesado impugne la exactitud de los datos, durante un plazo que permita la responsable verificar la exactitud de los mismos.
- Tratamiento ilícito- cuando el tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso.
- Reclamaciones- cuando el responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para el reconocimiento, ejercicio o defensa ante reclamaciones.

[9] https://edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-392021-whether-article-582g-gdpr-could_es

- Oposición- cuando el interesado se ha opuesto al tratamiento mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado.

Métodos para limitar el tratamiento de datos personales:

- Trasladar temporalmente los datos seleccionados a otro sistema de tratamiento.
- Impedir el acceso de usuarios a los datos personales seleccionados, o
- Retirar temporalmente los datos publicados de un sitio internet.

En los ficheros automatizados la limitación del tratamiento debe realizarse, en principio, por medios técnicos, de forma que los datos personales no sean objeto de operaciones de tratamiento ulterior ni puedan modificarse.

El hecho de que el tratamiento de los datos personales esté limitado debe indicarse claramente en el sistema.

7. Derecho a la portabilidad de los datos (nuevo derecho)

El interesado, de conformidad con el artículo 20 del RGPD, tendrá derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable de tratamiento, en un formato estructurado, de uso común o habitual y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado, cuando:

- El tratamiento esté basado en el consentimiento o en un contrato, y
- El tratamiento se efectúe por medios automatizados.

Ello sin perjuicio del ejercicio del derecho a la supresión.
En virtud a este derecho:

- Se aumenta la capacidad de trasladar, copiar o transmitir los datos personales fácilmente de un entorno informático a otro. Se trata de una forma avanzada del derecho de acceso.
- Debe alentarse a los responsables a crear formatos interoperables que permitan la portabilidad de los datos.
- El derecho del interesado a transmitir o recibir datos personales que lo conciernan no debe obligar al responsable a adoptar o mantener sistemas de tratamiento que sean técnicamente compatibles.
- El interesado debe tener derecho a que los datos personales se trasmitan directamente de un responsable del tratamiento a otro, cuando sea técnicamente posible.

Este derecho no se aplicará:

- Por su propia naturaleza, al tratamiento necesario para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable.

- Cuando la revelación de los datos personales vulnera los derechos de propiedad intelectual respecto del tratamiento de dichos datos personales.

Las Directrices sobre el derecho a la portabilidad de los datos del Grupo de Trabajo del Artículo 29 WP 242 rev.01, vienen a establecer que es una práctica recomendable que los responsables del tratamiento comiencen a desarrollar los medios que contribuyan a responder a las solicitudes de portabilidad de datos, como herramientas de descarga e interfaces de programación de aplicaciones. Deben garantizar que los datos personales se transmitan en un formato estructurado, de uso común y lectura mecánica, y se les debe alentar a que aseguren la interoperabilidad del formato de los datos proporcionados en el ejercicio de una solicitud de portabilidad.

No obstante, este derecho, por su propia naturaleza, no se puede aplicar cuando el tratamiento sea necesario para el cumplimiento de una misión de interés público o en el ejercicio de poderes públicos conferidos al responsable[10].

8. Derecho de oposición

Es el derecho del interesado a oponerse, en cualquier momento, por motivos relacionados con su situación particular, a que datos personales que le conciernan sean objeto de un tratamiento. Puede abarcar situaciones de todo tipo, como el derecho a oponerse a ser sometido a decisiones automatizadas, por situaciones particulares del propio interesado u oponerse a tratamientos posteriores de sus datos con fines de mercadotecnia directa.

En el marco de Consejo de Europa, nos encontramos con descripciones de gran calidad en la Recomendación sobre la elaboración de perfiles[11] y la Recomendación sobre la Mercadotecnia Directa[12]

No es un derecho absoluto, requiriendo de una ponderación de los motivos alegados tal y como se recogen en Asuntos como M.S c. Suecia[13], Leander c. Suecia[14] o Mosley c. el Reino Unido[15], donde el TEDH concluyó que no se había producido una violación del Convenio, aunque el derecho de oposición de los interesados no fuese reconocido en el derecho interno.

Este derecho debe comunicarse explícitamente al interesado, presentándose claramente y al margen de cualquier otra información.

Puede ejercitarse el derecho de oposición en los siguientes supuestos:

- Tratamientos de datos en interés público.
- De interés legítimo.
- Elaboración de perfiles sobre la base de dichas disposiciones anteriores.

[10] https://www.aepd.es/es/derechos-y-deberes/conoce-tus-derechos/derecho-la-portabilidad
[11] https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805cdd00
[12] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804bd336
[13] https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-58177%22]}
[14] https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-57519%22]}
[15] https://hudoc.echr.coe.int/eng-press#{%22fulltext%22:[%2248009/08%22]}

En estos supuestos, el responsable dejará de tratar los datos personales, salvo que acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado, o sea necesario para la formulación, el ejercicio o la defensa de reclamaciones.

Asimismo, cuando el tratamiento de datos personales tenga por objeto la mercadotecnia directa, el interesado tendrá derecho a oponerse en todo momento al tratamiento de los datos que le conciernan, incluida la elaboración de perfiles en la medida en que esté relacionada con la citada mercadotecnia[16]. En tales casos, los datos personales dejarán de ser tratados para dichos fines.

A más tardar en el momento de la primera comunicación con el interesado, la atención del derecho de oposición será informada explícitamente al interesado y será presentada claramente y al margen de cualquier otra información.

En el contexto de la utilización de servicios de la sociedad de la información, y no obstante lo dispuesto en la Directiva 2002/58/CE, el interesado podrá ejercer su derecho a oponerse por medios automatizados que apliquen especificaciones técnicas.

Cuando los datos personales se traten con fines de investigación científica o histórica o fines estadísticos, el interesado tendrá derecho, por motivos relacionados con su situación particular, a oponerse al tratamiento de datos personales que le conciernan, salvo que sea necesario para el cumplimiento de una misión realizada por razones de interés público.

Por ejemplo, en el supuesto de *«publicidad institucional»* remitida por una Administración pública u Órgano administrativo, sería también posible el ejercicio del derecho de oposición al tratamiento, sin necesidad de que el ciudadano afectado especificara ningún motivo concreto.

Finalmente, en caso de ejercicio del derecho de oposición por un afectado al tratamiento de sus datos personales con fines de investigación y estadísticos, la excepción al mismo sólo puede basarse en claras razones de interés público.

El ejercicio completo de este derecho impide al responsable continuar tratando los datos, sin embargo, las operaciones llevadas a cabo antes del ejercicio del derecho deberán entenderse legítimas.

Analizado el contenido del derecho, ¿cuál sería la diferencia con el derecho de supresión? A esta pregunta se puede responder brevemente de la siguiente forma: en el derecho de oposición estamos ante un tratamiento ilegítimo en apariencia o un tratamiento sobre el cual prevalecen los derechos del interesado, manifestando el mismo su disconformidad. Mientras que el derecho de supresión supone que se dejarán de utilizar una serie de datos personales sobre los cuales en su día hubo una base legal y justificada para su tratamiento.

9. Derecho a la limitación de las decisiones individualizadas automatizadas

Se trata del derecho de todo interesado a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfi-

[16] Resultan de interés en cuestiones de mercadotécnica: el Dictamen 2/2010 del Grupo de Trabajo del Artículo 29 sobre la publicidad basada en el comportamiento online, el Dictamen 5/2009, del Grupo de Trabajo del Artículo 29 sobre las redes sociales en línea y el Dictamen del SEPD sobre la «Estrategia europea para una Internet más adecuada para niños»

les, que produzca efectos jurídicos en él o le afecte significativamente de modo similar.

Dentro del Consejo de Europa, la Recomendación sobre la Elaboración de perfiles viene a establecer el derecho a los particulares interesados a oponerse a aquellas decisiones que sean tomadas exclusivamente por medios automatizados. Sin embargo, como veremos, el RGPD si permite estas actuaciones se concurren determinados requisitos.

La decisión individual automatiza podría definirse como aquella relativa a un individuo tomada en base al tratamiento de sus datos personales únicamente para una evaluación efectuada por medios automatizados.

En cuanto a la elaboración de perfiles podríamos describirla como toda forma de tratamiento automatizado de datos personales destinado a evaluar determinados aspectos personales propios de una persona física o a analizar o predecir en particular su rendimiento profesional, su situación económica, su localización, su estado de salud, sus preferencias personales, su fiabilidad o su comportamiento o ubicación.

Sin embargo, es lícito efectuar el tratamiento y tomar una decisión automatizada cuando:

- Está autorizada por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado.
- Sea necesaria para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento.
- Se basa en el consentimiento explícito del interesado.

Las decisiones sobre la base de tratamientos automatizados no se podrán basar en las categorías especiales de datos personales, salvo consentimiento explícito o que sea necesario por Ley o interés público. Y el riesgo de que se tome una decisión potencialmente dañina sin intervención

El responsable o la ley que autorice el tratamiento adoptará las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, como mínimo el derecho a obtener intervención humana por parte del responsable, a expresar su punto de vista y a impugnar la decisión.

Un ejemplo de tratamiento -que tiene como fin la adopción de una decisión referida a un ciudadano basada únicamente en un tratamiento automatizado de sus datos personales-, concurre cuando un programa informático propone una decisión que afecta al ciudadano, realizando un análisis de sus datos de carácter personal a fin de evaluar su capacidad económica, su modo de vida, su rendimiento laboral, o su capacidad de crédito.

10. Excepciones o limitaciones del ejercicio de derechos

En el asunto 9248/81 Leander c. Suecia, el TEDH ya llegó a la conclusión de que el derecho a acceder a los datos personales almacenados por las autoridades públicas podría quedar limitado si se concurrían determinadas circunstancias de

manera que no se vulneraban los artículos 8, 10 o 13 del Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales.

El artículo 11.1 del Convenio 108 + establece que la solicitud de acceso de las personas interesadas puede verse limitada cuando dicha excepción esté prevista por la ley, respete la esencia de los derechos y libertades fundamentales y constituya una medida necesaria y proporcionada en una sociedad democrática para proteger los intereses nacionales, para proteger al interesado o los derechos y libertades fundamentales de los demás, en particular la libertad de expresión.

Del mismo modo, el artículo 23 RGPD contempla la posibilidad de que el derecho a la información y el derecho a la protección de datos puedan verse limitados si el contenido esencial de los mismos no queda afectado, y sea necesario y proporcionado para salvaguardar:

- La seguridad del Estado.
- La defensa.
- La seguridad pública.
- La prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluida la protección frente a amenazas a la seguridad pública y su prevención.
- Otros objetivos importantes de interés público general de la Unión o de un Estado miembro, en particular un interés económico o financiero importante de la Unión o de un Estado miembro, inclusive en los ámbitos fiscal, presupuestario y monetario, la sanidad pública y la seguridad social.
- La protección de la independencia judicial y de los procedimientos judiciales.
- La prevención, la investigación, la detección y el enjuiciamiento de infracciones de normas deontológicas en las profesiones reguladas.
- Una función de supervisión, inspección o reglamentación vinculada, incluso ocasionalmente, con el ejercicio de la autoridad pública en los casos contemplados en las letras a) a e) y g).
- La protección del interesado o de los derechos y libertades de otros.
- La ejecución de demandas civiles.

En todo caso, cualquier limitación en este sentido contendrá disposiciones específicas relativas a:

- La finalidad del tratamiento o de las categorías de tratamiento.
- Las categorías de datos personales de que se trate.
- El alcance de las limitaciones establecidas.
- Las garantías para evitar accesos o transferencias ilícitos o abusivos.
- La determinación del responsable o de categorías de responsables.
- Los plazos de conservación y las garantías aplicables, habida cuenta de la naturaleza, alcance y objetivos del tratamiento o las categorías de tratamiento.
- Los riesgos para los derechos y libertades de los interesados, y.
- El derecho de los interesados a ser informados sobre la limitación, salvo si puede ser perjudicial a los fines de esta.

Además, pueden establecerse excepciones respecto a tratamientos de datos personales realizados con fines periodísticos o con fines de expresión académica, artística o literaria, y con fines de archivo en interés público.

En estos casos resulta útil como elemento de consulta las *«Directrices 10/2020, sobre restricciones de derechos bajo el Artículo 23 del RGP*D»[17] del Comité Europeo de Protección de Datos cuyas conclusiones vienen a redundar en estas cuestiones señalando que:

- El artículo 23 del RGPD permite, en condiciones específicas, que un legislador nacional o de la Unión restrinja, mediante una medida legislativa, el alcance de las obligaciones y derechos previstos en los artículos 12 a 22 y el artículo 34, así como el artículo 5 del RGPD, cuando tal restricción respete la esencia de los derechos y libertades fundamentales y sea una medida necesaria y proporcionada en una sociedad democrática para salvaguardar, entre otros, importantes objetivos de interés público general de la Unión o de un Estado miembro.
- Estas restricciones deben cumplir los requisitos establecidos en el artículo 23 del RGPD y los Estados miembros que dicten medidas legislativas que establezcan esas restricciones y los responsables del tratamiento que las apliquen deben ser conscientes del carácter excepcional de estas restricciones.
- La prueba de proporcionalidad debe llevarse a cabo antes de introducir en la legislación de la Unión o de los Estados miembros cualquier restricción a los derechos de los interesados.
- Del mismo modo, las Autoridades independientes de control deben ser consultadas antes de la adopción de las medidas legislativas que establecen las restricciones y de manera que puedan ejercer sus poderes para hacer cumplir la normativa de protección de datos.
- Y como cuestión relevante, cabe incidir en que una vez que se levantan las restricciones, el responsable del tratamiento debe permitir que los interesados ejerzan sus derechos.

Por último, señalar que todos estos derechos cabe interpretarlos siempre en el contexto de las particularidades contenidas en otras normas o disposiciones. A modo de ejemplo, es importante citar las peculiaridades contenidas en el artículo 28 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

Singularmente, los apartados 1 a 3 resultan clarificadores. Señalando que:

> *«1. Los interesados deberán aportar al procedimiento administrativo los datos y documentos exigidos por las Administraciones Públicas de acuerdo con lo dispuesto en la normativa aplicable. Asimismo, los interesados podrán aportar cualquier otro documento que estimen conveniente.*
>
> *2. Los interesados tienen derecho a no aportar documentos que ya se encuentren en poder de la Administración actuante o hayan sido elaborados por*

[17] «Guidelines 10/2020 on restrictions under Article 23 GDPR Version 2.0, Adopted on 13 October 2021»

cualquier otra Administración. La administración actuante podrá consultar o recabar dichos documentos salvo que el interesado se opusiera a ello. No cabrá la oposición cuando la aportación del documento se exigiera en el marco del ejercicio de potestades sancionadoras o de inspección.

Las Administraciones Públicas deberán recabar los documentos electrónicamente a través de sus redes corporativas o mediante consulta a las plataformas de intermediación de datos u otros sistemas electrónicos habilitados al efecto.

Cuando se trate de informes preceptivos ya elaborados por un órgano administrativo distinto al que tramita el procedimiento, estos deberán ser remitidos en el plazo de diez días a contar desde su solicitud. Cumplido este plazo, se informará al interesado de que puede aportar este informe o esperar a su remisión por el órgano competente.

3. Las Administraciones no exigirán a los interesados la presentación de documentos originales, salvo que, con carácter excepcional, la normativa reguladora aplicable establezca lo contrario.

Asimismo, las Administraciones Públicas no requerirán a los interesados datos o documentos no exigidos por la normativa reguladora aplicable o que hayan sido aportados anteriormente por el interesado a cualquier Administración. A estos efectos, el interesado deberá indicar en qué momento y ante qué órgano administrativo presentó los citados documentos, debiendo las Administraciones Públicas recabarlos electrónicamente a través de sus redes corporativas o de una consulta a las plataformas de intermediación de datos u otros sistemas electrónicos habilitados al efecto, salvo que conste en el procedimiento la oposición expresa del interesado o la ley especial aplicable requiera su consentimiento expreso. Excepcionalmente, si las Administraciones Públicas no pudieran recabar los citados documentos, podrán solicitar nuevamente al interesado su aportación.»

11. Referencia a los derechos relativos a los datos de personas fallecidas

El artículo 3 de la LOPDGDD se refiere al acceso a datos de personas fallecidas. Así, las personas vinculadas al fallecido por razones familiares o de hecho, así como sus herederos que acrediten tal condición mediante cualquier medio válido conforme a Derecho, podrán dirigirse al responsable o encargado al objeto de solicitar el acceso a los datos personales de aquella y, en su caso, su rectificación o supresión, excepto si el citado fallecido lo hubiese prohibido expresamente o así lo establezca una ley.

También lo puede solicitar el albacea, así como aquella persona o institución a la que el fallecido hubiese designado expresamente.

Si se tratase de fallecimiento de menores, estas facultades podrán ejercerse también por sus representantes legales o, en el marco de sus competencias, por el Ministerio Fiscal, que podrá actuar de oficio o a instancia de cualquier persona física o jurídica interesada.

En caso de fallecimiento de personas con discapacidad, estas facultades también podrán ejercerse, además de por quienes señala el párrafo anterior, por quienes hubiesen sido designados para el ejercicio de funciones de apoyo.

II. ESPECIFICIDADES RESPECTO A LA NORMATIVA REGULADORA DE LA PROTECCIÓN DE DATOS PERSONALES CON FINALIDAD DE PREVENCIÓN, INVESTIGACIÓN Y DETECCIÓN DE INFRACCIONES PENALES

1. Derechos comunes con el RGPD

Aún a riesgo de que resulte repetivio con respecto a los derechos vistos anteriormente en referencia al RGPD, no está de más señalar lo que establece la LOPDP:

En concreto, en este epígrafe se detalla el contenido del Capítulo III de la citada Ley Orgánica, que comprende los artículos 20 a 26.

Como condiciones generales de ejercicio cabe señalar las siguientes:

- Es obligación del responsable del tratamiento facilitar al interesado toda la información relacionada con sus derechos. Debe hacerlo de forma concisa, inteligible, de fácil acceso, y con lenguaje claro y sencillo para todas las personas.
- La información será facilitada por cualquier medio adecuado, incluido los electrónicos, procurando utilizar el mismo medio empleado en la solicitud. Se informará por escrito, sin dilación indebida sobre el curso dado a su solicitud. En caso de que transcurra un mes desde su presentación no se ha resuelto expresamente y notificada al interesado, se entenderá desestimada.

- La información será gratuita.
- El responsable podrá inadmitir a trámite de manera motivada cuando considere que la solicitud es manifiestamente infundada o excesiva por repetitiva. Se considerará repetitiva la solicitud cuando se realicen tres sobre el mismo supuesto en el plazo de seis meses, salvo que exista legítima causa para ello.
- El interesado podrá actuar en su propio nombre o por medio de representantes, siempre que tenga capacidad de obrar. Cuando el responsable del tratamiento tenga dudas razonables acerca de la identidad de la persona física que formula la solicitud le requerirá para que facilite la información complementaria necesaria en el plazo de 10 días desde la fecha en que el interesado facilite la información solicitada, transcurrido el cual sin que se aporte la información complementaria se le tendrá por desistido en su solicitud.

La información que el responsable del tratamiento debe poner a disposición del interesado sería la que se relaciona:

- La identidad y los datos de contacto del responsable del tratamiento y sus datos de contacto.
- Los datos de contacto del delegado de protección de datos, en su caso.
- Los fines del tratamiento a que se destinen los datos personales.
- El derecho a presentar una reclamación ante la autoridad de control y los datos de contacto de la misma.

- El derecho a solicitar del responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación, supresión o la limitación de su tratamiento.

Atendiendo a las circunstancias del caso concreto, se tiene que facilitar al interesado la información sobre:

- La base jurídica del tratamiento.
- El plazo durante el cual se conservarán los datos personales o, cuando esto no sea posible, los criterios utilizados para determinar ese plazo.
- Las categorías de destinatarios de los datos personales, en particular en terceros países u organizaciones internacionales.
- Cualquier otra información necesaria, en especial, cuando los datos personales se hayan recogido sin conocimiento del interesado.

En cuanto al derecho de acceso cabe indicar que, en virtud de la DDP y la LOPDP, como particularidad al régimen del RGPD, tendrá derecho acceder a la comunicación de los datos personales objeto de tratamiento, así como cualquier información disponible sobre su origen, sin revelar la identidad de ninguna persona física, en especial en el caso de fuentes confidenciales.

Cuando el responsable trate una gran cantidad de información relativa al interesado y éste no especifique si se refiere a todos o a una parte, el responsable podrá requerir al interesado que concrete la solicitud en el plazo de 10 días.

En cuanto a los derechos de rectificación, supresión y limitación, no existirían especificidades que reseñables que podamos señalar en la descripción de estos derechos desde ambos prismas, si bien, existen algunos que no tienen aplicación directa en este campo.

Los diferentes derechos a aplicar se pueden resumir de manera esquemática en el siguiente cuadro:

PREVIO AL RGPD	RGPD	DIRECTIVA 680
ACCESO	ACCESO	ACCESO
RECTIFICACIÓN	RECTIFICACIÓN	RECTIFICACIÓN
CANCELACIÓN	SUPRESIÓN	SUPRESIÓN
OPOSICIÓN	OPOSICIÓN	X
X	LIMITACIÓN	LIMITACIÓN
X	PORTABILIDAD	X
X	DERECHO A NO SER OBJETO DE DECISIONES INDIVIDUALES AUTOMATIZADAS	DERECHO A NO SER OBJETO DE DECISIONES INDIVIDUALES AUTOMATIZADAS
X	DERECHO DE INFORMACIÓN	DERECHO DE INFORMACIÓN

Como puede apreciarse del cuadro expuesto los derechos son similares, si bien la Directiva no recoge la posibilidad de ejercer el derecho a la portabilidad dado que este derecho, por su propia naturaleza, no se puede aplicar cuando el tratamiento sea necesario para el cumplimiento de una misión de interés público o en el ejercicio de poderes públicos conferidos al responsable. Así como tampoco refleja la posibilidad de ejercitar el derecho de oposición. Este derecho viene actualmente regulado en el artículo 21 del RGPD y sería aquel que permite al interesado oponerse (negarse), en cualquier momento, por motivos relaciones con su situación particular, a que sus datos personales sean objeto de un tratamiento, lo cual, dada la finalidad específica de los tratamientos de la Directiva lo convierte en incompatible con ésta.

Señala igualmente que los interesados tendrán derecho a ser indemnizados por el responsable del tratamiento (autoridades competentes), o por el encargado del tratamiento, cuando forme parte del sector público, cuando sufran daño o lesión en sus bienes o derechos como consecuencia del incumplimiento de lo dispuesto en la normativa que regule el tratamiento de los datos con fines policiales. En el caso de que el responsable sea una autoridad pública administrativa, la responsabilidad se exigirá de acuerdo con la legislación reguladora del régimen de responsabilidad previsto en la normativa sobre el procedimiento administrativo común y sobre el régimen jurídico del sector público o la especial que lo regule.

Por el contrario, los interesados que sufrieran daño o lesión en sus bienes o derechos por parte de un encargado del tratamiento que no forme parte del sector público, también tendrán derecho a ser indemnizados.

Si bien, la reclamación de los interesados se formulará, en todo caso, conforme al procedimiento establecido en la legislación aplicable a cada supuesto.

2. Análisis de las peculiaridades previstas en la normativa específica (LOPDP)

Es un tema de suma importancia la implementación de las restricciones a los derechos de información, acceso, rectificación, supresión y a la limitación de tratamiento en el campo de la LOPDP ya que es necesario establecer a priori y en todo caso un estudio del juicio de proporcionalidad en toda su extensión para que los derechos, bienes jurídicos e intereses implicados no sufran un perjuicio injustificado.

El responsable del tratamiento podrá aplazar, limitar u omitir la información relacionada con sus derechos, así como denegar total o parcialmente las solicitudes de ejercicio de los derechos de acceso, rectificación, supresión y limitación, siempre que resulte necesario y proporcional para:

- Impedir que se obstaculicen indagaciones, investigaciones o procedimientos judiciales.
- Evitar que se cause perjuicio a la prevención, detección, investigación y enjuiciamiento de infracciones penales o a la ejecución de sanciones penales.
- Proteger la seguridad pública, la Seguridad Nacional o los derechos y libertades de otras personas.

En estos casos de restricción, el responsable informará por escrito al interesado sin dilación indebida y en todo caso en el plazo de un mes desde que tenga conocimiento de dicha restricción de las razones de la misma, así como de las posibilidades de presentar una reclamación ante la autoridad de protección de datos, sin perjuicio de las restantes acciones judiciales que pueda ejercer en virtud de lo establecido en la LO.

Así, en los casos de aplazamiento, limitación u omisión de la información a que se refiere el artículo 21 o una restricción del ejercicio de los derechos contemplados en los artículos 22 y 23, el interesado podrá ejercer sus derechos a través de la autoridad de protección de datos competente. El responsable del tratamiento informará al interesado de esta posibilidad.

Las razones de la restricción podrán ser omitidas o ser sustituidas por una redacción neutra cuando la revelación de los motivos de la restricción pueda poner en riesgo los fines a los que nos hemos referido antes.

El responsable del tratamiento documentará los fundamentos de hecho o de derecho en los que se sustente la decisión denegatoria del ejercicio del derecho de acceso. Dicha información estará a disposición de las autoridades de protección de datos. El interesado podrá ejercer sus derechos a través de estos, quien, en caso de así hacerlo, informará al interesado, al menos, de la realización de todas las comprobaciones necesarias o la revisión correspondiente y de su derecho a interponer recurso contencioso-administrativo.

En el ámbito policial y judicial en muchas ocasiones las autoridades competentes deben velar por que se protejan todos los derechos en juego que puedan tener las personas interesadas o afectadas. Los derechos colectivos e individuales que tienen por objeto proteger y garantizar las FCS y el resto de las autoridades competentes, en muchas ocasiones, se contraponen o complementan con derechos individuales como la tutela efectiva de los jueces y tribunales sin que pueda producir indefensión, el derecho a la defensa y a la asistencia de letrado, a ser informados de la acusación formulada, a un proceso con todas las garantías, uso de pruebas pertinentes para la defensa, presunción de inocencia, etc.

Este magnífico equilibrio democrático facilita herramientas a todos las personas y agentes que tienen que cumplir con sus misiones en este marco, por lo que es importante señalar que ningún derecho es absoluto y que todos puede ser modulados por la concurrencia de otros que posibilitan la convivencia y la vida en sociedad.

La cuestión no es baladí y no queda circunscrita al ámbito policial, sino que el propio RGPD y la LOPDGDD lo incorporan como un elemento fundamental en su aplicación. Los artículos 5 y 23 del reglamento permiten limitaciones para que los responsables o encargados restrinjan, en base a un soporte legal, el alcance de sus obligaciones y de los derechos de los interesados y el 8 de la ley orgánica establece la forma de tratamiento de los datos por obligación legal, interés público o ejercicio de poderes públicos de manera se fijen las condiciones generales de cada tratamiento, los datos, las cesiones y condiciones especiales como la adopción de medidas de seguridad o cualquier otra de las recogidas en el capítulo IV del reglamento.

Imaginemos que una persona que sospecha que puede estar siendo investigada por las Fuerzas y Cuerpos de Seguridad y que, una vez cada dos o tres meses, solicita el acceso a los datos personales que tengan estas autoridades compe-

tentes en algunos de sus ficheros de actividades de tratamiento. En el caso de que se faciliten los datos puede desbaratar los fines de investigación y, del mismo modo, sucedería en el caso de que se niegue la información ya que la persona puede deducir que efectivamente está siendo investigada. Por este motivo, deben articularse un sistema que permita garantizar la efectividad de las investigaciones y a la vez de cobertura al ejercicio de los derechos de las personas.

Conforme a la LOPDP, el responsable del tratamiento de la autoridad competente podrá aplazar, limitar u omitir la siguiente información, para el ejercicio de los derechos por parte de los interesados:

- La base jurídica del tratamiento.
- El plazo durante el cual se conservarán los datos personales o, cuando esto no sea posible, los criterios utilizados para determinar ese plazo.
- Las categorías de destinatarios de los datos personales, cuando corresponda, en particular, los establecidos en Estados que no sean miembros de la Unión Europea u organizaciones internacionales.
- Cualquier otra información necesaria, en particular, cuando los datos personales se hayan recogido sin conocimiento del interesado.

Asimismo, podrá denegar, total o parcialmente, las solicitudes de ejercicio de los derechos acceso, rectificación, supresión de datos personales y a la limitación de su tratamiento, siempre que, teniendo en cuenta los derechos fundamentales y los intereses legítimos de la persona afectada, resulte necesario y proporcional para la consecución de los siguientes fines:

- Impedir que se obstaculicen indagaciones, investigaciones o procedimientos judiciales.
- Evitar que se cause perjuicio a la prevención, detección, investigación o enjuiciamiento de infracciones penales o a la ejecución de sanciones penales.
- Proteger la seguridad pública.
- Proteger la Seguridad Nacional.
- Proteger los derechos y libertades de otras personas.

En caso de restricción de los derechos acceso, rectificación, supresión de datos personales y a la limitación de su tratamiento, el responsable del tratamiento de la autoridad competente informará por escrito al interesado sin dilación indebida, y en todo caso en el plazo que se determine legalmente, de dicha restricción, de las razones de la misma, así como de las posibilidades de presentar una reclamación ante la autoridad de protección de datos, sin perjuicio de las restantes acciones judiciales que pueda ejercer en virtud de lo dispuesto en esta ley orgánica.

Este responsable del tratamiento documentará los fundamentos de hecho o de derecho en los que se sustente la decisión denegatoria del ejercicio del derecho de acceso. Dicha información, previa petición, estará a disposición de las autoridades de protección de datos, conforme a la normativa específica aplicable a cada caso.

Otra cuestión que ya se ha comentado, sería la aplicación del deber de colaboración derivado del artículo 7 de la LOPDP de los distintos responsables y la previsión de que no se informe al interesado de determinados tratamientos cuan-

do estos se dirijan a trasladar datos a las autoridades competentes. Esto resulta obvio, fundamental y muy importante puesto que con la legislación anterior no se dejaba muy claro cómo debían comportarse los responsables ante estas solicitudes de cesión, acceso o transmisión de los datos.

Imaginemos por un momento que la policía judicial en la realización de sus investigaciones previas de carácter propio o incluso ya judicializadas solicita información formal y motivadamente a una entidad (gran superficie o similar) sobre determinados movimientos realizados de una persona a la que se le atribuye la comisión de un ilícito penal. Si los responsables, en virtud del derecho de información del interesado le trasladan que sus datos personales se han cedido a la policía judicial o al juzgado de instrucción se daría al traste con la investigación llevada a cabo y no permitiría cumplir con las finalidades específicas de estos tratamientos con fines policiales.

Entonces, ¿está claro que la policía judicial puede pedir estos datos en sus investigaciones, que no es necesario el consentimiento ni informar al interesado? Dadas las competencias de la misma y la finalidad del tratamiento, la respuesta es claramente afirmativa.

Esto lo ha valorado y corroborado la AEPD en varios informes que, aunque a día de hoy pueden quedar un poco desfasados ante la entrada en vigor de la LOPDP, resulta interesante estudiar los fundamentos que se señalaban para legitimar los tratamientos en un sistema principalmente basado en el consentimiento:

> *"..., a nuestro juicio, a los miembros de la Policía Judicial para la obtención y tratamiento de los datos requeridos, lo que llevará aparejada la procedencia de la cesión instada, siempre y cuando la Policía Judicial, cumplan las siguientes condiciones, que han sido reiteradas por la Agencia Española de Protección de datos:*
>
> *a) Que quede debidamente acreditado que la obtención de los datos resulta necesaria para la prevención de un peligro real y grave para la seguridad pública o para la represión de infracciones penales y que, tratándose de datos especialmente protegidos, sean absolutamente necesarios para los fines de una investigación concreta.*
>
> *b) Que se trate de una petición concreta y específica, al no ser compatible con lo señalado anteriormente el ejercicio de solicitudes masivas de datos.*
>
> *c) Que la petición se efectúe con la debida motivación, que acredite su relación con los supuestos que se han expuesto.*
>
> *d) Que, en cumplimiento del artículo 22.4 de la Ley Orgánica 15/1999, los datos sean cancelados «cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento».*

Con referencia a la última de las conclusiones señaladas, debe indicarse que, tratándose de actuaciones llevadas a cabo en el ámbito de las competencias consagradas en el apartado a) del artículo 549.1 de la Ley Orgánica del Poder Judicial, encontrándose por ello la Policía Judicial obligada a dar cuenta de los hechos a la Autoridad Judicial y Fiscal de forma inmediata, deberá procederse a la destrucción del registro de los datos obtenidos, una vez producida esa comunicación.

A mayor abundamiento, debe recordarse que, conforme dispone el artículo 11.2 d) de la LOPD, procederá la cesión si ésta tiene por destinatario al Minis-

terio Fiscal o los Jueces o Tribunales, lo que, conforme se ha señalado, ocurre en el presente supuesto, dada la obligación de los miembros de la Policía Judicial de poner los datos que hayan sido obtenidos en conocimiento de la Autoridad Judicial competente para conocer la denuncia o Fiscal. Por ello, la cesión solicitada tendrá amparo no sólo en el artículo 22.2 de la citada Ley Orgánica de 1999, sino también en el propio artículo 11.2 d) de la misma.

En virtud de todo lo cual, cabe concluir que procede la cesión de los datos que solicite la Policía Judicial, bien por aplicación del artículo 11.2 d), bien del citado artículo 22, no obstante, en este último supuesto, la solicitud deberá cumplir las condiciones manifestadas anteriormente.

Lo mismo ocurre con el acceso de las FCS a los padrones municipales. La Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local establece en su artículo 16.3 que:

> *«Los datos del Padrón Municipal se cederán a otras Administraciones públicas que lo soliciten sin consentimiento previo al afectado solamente cuando les sean necesarios para el ejercicio de sus respectivas competencias, y exclusivamente para asuntos en los que la residencia o el domicilio sean datos relevantes. También pueden servir para elaborar estadísticas oficiales sometidas al secreto estadístico, en los términos previstos en la Ley 12/1989, de 9 de mayo, de la Función Estadística Pública y en las leyes de estadística de las comunidades autónomas con competencia en la materia.»;*

Por otro lado, la LOPD en su disposición adicional segunda, establecía asimismo que:

> *«1. La Administración General del Estado y las Administraciones de las Comunidades Autónomas podrán solicitar al Instituto Nacional de Estadística, sin consentimiento del interesado, una copia actualizada del fichero formado con los datos del nombre, apellidos, domicilio, sexo y fecha de nacimiento que constan en los padrones municipales de habitantes y en el censo electoral correspondientes a los territorios donde ejerzan sus competencias, para la creación de ficheros o registros de población. 2. Los ficheros o registros de población tendrán como finalidad la comunicación de los distintos órganos de cada Administración pública con los interesados residentes en los respectivos territorios, respecto a las relaciones jurídico administrativas derivadas de las competencias respectivas de las Administraciones públicas.»*

Como puede verse ambos preceptos son algo contradictorios puesto que la LOPD permitía que se traten más datos que los previstos en la LBRL, si bien legitima legalmente para que las FCS soliciten y accedan los datos que sean necesarios en cada caso de investigación concreta, no limitándose a un archivo o al acceso a todos los archivos siempre que dicha información sea necesaria para el desarrollo de sus concretas competencias, el tratamiento sea para fines policiales y se acomode a los requisitos de seguridad y confidencialidad que se imponen en la normativa de protección de datos.

Sin embargo, la LOPDP ha venido a aclarar esta situación con su base de legitimación, el deber de colaboración y la disposición adicional cuarta:

«Ficheros y Registro de Población de las Administraciones Públicas. 1. Las autoridades competentes podrán solicitar al Instituto Nacional de Estadística y a los órganos estadísticos de ámbito autonómico, sin consentimiento del interesado, una copia actualizada del fichero formado con los datos del documento de identidad, nombre, apellidos, domicilio, sexo y fecha de nacimiento que constan en el padrón municipal de habitantes y en el censo electoral correspondiente a los territorios donde ejerzan sus competencias. Esta solicitud deberá estar motivada en base a cualquiera de los fines de prevención, detección, investigación y enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública.

2. Los datos obtenidos tendrán como único propósito el cumplimiento de los fines de prevención, detección, investigación y enjuiciamiento de infracciones penales o de ejecución de sanciones penales, así como de protección y de prevención frente a las amenazas contra la seguridad pública y la comunicación de estas autoridades con los interesados residentes en los respectivos territorios, respecto a las relaciones jurídico-administrativas derivadas de las competencias respectivas.»

En relación con todos estos supuestos, la posición más reciente y relevante sería el contenido del informe del Gabinete Jurídico de la AEPD número N/REF: 0030/2021[18], que se centra sobre la en la adecuación al marco jurídico vigente respecto del acceso por parte de las FCS en lo sucesivo, a la información de la que disponen las Operadoras de Telecomunicaciones derivado de los servicios que prestan y de las posibilidades de que conforme a la ley puedan mejorar el sistema para la lucha contra el SIM Swapping.

Entre otras importantes conclusiones, concluye este instrumento con la premisa siguiente:

«Por lo tanto, las operadoras de telecomunicaciones están obligadas a proporcionar la información sobre la vinculación entre el IMEI y el IMSI, -siempre que no se encuentre vinculado a un proceso de comunicación, en cuyo caso se necesitara autorización judicial- así como los datos conexos al proceso de duplicación de la tarjeta SIM, no solo por lo indicado en el artículo 588 ter m) de la LECrim, sino también al amparo del deber de colaboración que se acaba de indicar, y sin perjuicio de que la comunicación de los datos se realizaría al amparo del artículo 6.1 c) del RGPD.

Por otra parte, debe recordarse que los responsables del tratamiento -las autoridades competentes- están sometidos a las obligaciones referidas a los plazos de conservación y revisión (artículo 8) y, entre otras, a las relativas a la «protección de datos desde el diseño y por defecto» previstas en el artículo 28 y la «seguridad del tratamiento» referida en el artículo 37 de la citada ley orgánica.

Por lo tanto, y en relación con el tratamiento objeto de análisis en la presente consulta, debe indicarse que del lado de las operadoras encuentra su legitimación en el artículo 6.1 c) del RGPD, y una vez que las FCS y/o el Ministerio Fiscal dispongan de los datos, dicho tratamiento se somete a la Ley

[18] https://www.aepd.es/es/documento/2021-0030.pdf

Orgánica 7/2021, de 26 de mayo y por tanto, deberán cumplirse los principios referidos en el artículo 6, y en especial los de limitación de la finalidad y minimización (apartados b) y c)).»

2.1. Régimen especial como consecuencia de investigaciones y procesos penales

Este aspecto recogido en la LOPDP no es una cuestión baladí y es una de las cuestiones principales a la hora de interpretar la posible aplicación de derechos de las personas interesadas en los tratamientos que se están llevando a cabo en investigaciones o procesos en el ámbito penal.

La Sentencia del Tribunal Supremo 312/2021, Recurso 10588/2020, de 7 de abril de 2021, en el que se analizan estas cuestiones, sobre todo en virtud del contenido de la Directiva 2012/13/UE del Parlamento Europeo y del Consejo, de 22 de mayo de 2012, relativa al derecho a la información en los procesos penales, que recoge en su artículo 6 el derecho de todo sospechoso o acusado a ser informado sobre la infracción penal que se le atribuye, debiendo ser informado con un grado de detalle que permita el ejercicio efectivo de los derechos de defensa y en su artículo 7 el derecho de acceso a los materiales del expediente.

El Alto Tribunal detalla por un lado que:

«Esta Sala ya ha expresado en su STS 795/2014, de 20 de noviembre, que la salvaguardia de la equidad del proceso y de la preparación de la defensa, que la Directiva 2012/13/UE garantiza al reconocer el derecho de todo encausado a acceder a la totalidad de las pruebas materiales que estén en posesión de las autoridades competentes (art. 7.2 de la Directiva), se proyecta sobre la totalidad de las pruebas materiales, a favor o en contra; si bien el derecho no abarca al conocimiento de las fuentes o el origen de la investigación estrictamente policial. Repasábamos en aquella resolución los antecedentes normativos históricos existentes al respecto. Concretamente decíamos "Ya la Real Orden de 4 de octubre de 1861, extendiendo lo dispuesto en las de 6 de julio de 1850 y 31 del propio mes de 1851, dispensaba a los comisarios e inspectores de policía de revelar en juicio el nombre de sus confidentes, y lo mismo se vino previniendo en disposiciones posteriores que reglamentaron los servicios de policía y vigilancia; también la jurisprudencia de esta Sala (SSTS de 7 de octubre de 1889 , 13 de noviembre de 1890 , 9 de abril de 1968 , 22 de marzo de 1986 ó 635/2008 de 3 de octubre) afirmó la impertinencia de las preguntas dirigidas a estos fines 'salvo determinadas circunstancias'; y el acuerdo sobre principios básicos de actuación de las Fuerzas y Cuerpos de Seguridad del Estado, publicado por Orden de 30 de septiembre de 1981 con carácter provisional hasta que se dictare la norma legal de rango adecuado, adoptó la Resolución 690 del Consejo de Europa relativa a la Declaración sobre la Policía, estableciendo -principio número quince- que los miembros de dichos Cuerpos no están obligados a revelar la identidad o circunstancias de aquellas personas que colaboran con ellos 'salvo cuando su actuación hubiera dado lugar a la comisión de hechos punibles'. Congruentemente, la Ley Orgánica de Fuerzas y Cuerpos de Seguridad dedica un capítulo, a modo de código deontológico, a los que titula 'Principios básicos de actuación', que sigue las

pautas marcadas en la citada resolución del Consejo de Europa, y en el 'Código de conducta para los funcionarios encargados de hacer cumplir la ley' de la Asamblea de las Naciones Unidas, imponiendo a los miembros de los cuerpos policiales un 'absoluto' respeto a la Constitución -que por mor del Recurso Nº: 10588/2020 principio de igualdad no consiente parcelas de inmunidad-, donde asimismo les sigue eximiendo de revelar las fuentes de información 'salvo que el ejercicio de sus funciones o las disposiciones de la ley les imponga actuar de otra manera' (artículo 5.1 y 5)". Asimismo, recordábamos en aquella sentencia que la doctrina jurisprudencial del TEDH ha admitido la legalidad de la utilización de fuentes confidenciales de información, siempre que se utilicen exclusivamente como medios de investigación y no tengan acceso al proceso como prueba de cargo (Asuntos Kostovski , de 20 de noviembre de 1989 -& 44-, o Windisch , de 27 de septiembre de 1990 -& 30-).»

Por otro lado, recuerda:

«El derecho a conocer la información que pueda resultar relevante para el material probatorio no es de configuración absoluta y sin modulación.», además de que*: «En modo alguno el derecho abarca a conocer el contenido de la investigación preprocesal, cuyo resultado final, al tener valor de denuncia o de mero objeto de la prueba (art. 297 LECRIM), sólo sirve para el arranque del proceso penal y se materializa como referencia inaugural para el ejercicio del derecho de defensa en la forma procesalmente prevista.»* y *«Pero tampoco existe un derecho a conocer o desvelar los métodos y las técnicas de investigación policial desarrolladas en nuestros límites territoriales, como no lo hay tampoco a conocer la identidad de los agentes que hayan intervenido en la investigación, cuando no tiene una repercusión legal sobre el material probatorio en el que pueda fundarse una eventual acusación. Los investigados sometidos a proceso penal carecen de un derecho que les ampare a desvelar los puntos de apostamiento policial, o la identidad de los confidentes, o la información recabada mediante técnicas de criminalística que perderían su eficacia si se divulgaran masivamente. No existe un derecho a conocer los instrumentos y materiales concretos de los que se dispuso la policía para la investigación y que podrían quedar desprovistos de eficacia para intervenciones futuras. Tampoco hay un derecho a conocer las indagaciones de otros delitos que puedan atribuirse a los mismos sospechosos pero que estén todavía en proceso de confirmación policial, menos aún si consideramos que, en su caso, deberán ser objeto de un procedimiento de persecución penal independiente (art. 17.1 LECRIM). Como no resulta tampoco asumible que se conozcan aquellas investigaciones que ni siquiera afectan a los sometidos a proceso y que pueden arruinar otras actuaciones policiales de obligada persecución de la criminalidad. Sólo cuando una de las partes presente indicios fundados de que la actuación policial o preprocesal puede haber quebrantado sus derechos fundamentales, incurrido en irregularidades, o discurrido de un modo que pueda afectar a la validez de la prueba o del procedimiento penal, así como cuando aporte indicios de coexistir circunstancias en la investigación que puedan afectar a la fuerza incriminatoria del material probatorio, se justifica, por los principios de equilibrio y defensa, autorizar tal prospección, siempre limitada a los estrictamente necesario y bajo control judicial.»*

En base a estos presupuestos el TS emite las importantes conclusiones que se enumeran:

a. Las partes personadas, y en particular los encausados, tienen derecho a conocer el contenido íntegro de las actuaciones procesales, sin más excepción que la derivada de su declaración de secreto (art. 302 LECRIM).
b. Este derecho se extiende a conocer actos jurisdiccionales limitativos de derechos fundamentales realizados en otro procedimiento judicial, cuando de su legitimidad dependa la validez del medio probatorio que le afecta y no se hayan ya incorporado al proceso (arts. 579 bis y 588 bis i de la LECRIM).
c. El derecho de las partes a conocer y examinar las actuaciones procesales, plasmado en los artículos 118, 627, 780.1 y 784.1 de la LECRIM no faculta conocer la investigación pre-procesal que no se haya reflejado en las actuaciones.
d. Excepcionalmente, cuando se presenten indicios fundados de concurrir circunstancias que comprometen la validez de la prueba o que razonablemente pueden condicionar su credibilidad o su capacidad indicativa, afectando con ello al derecho de defensa de las pretensiones de las partes, estas pueden solicitar de la Autoridad Judicial competente que incorpore, únicamente, los extremos concretos de la investigación prejudicial que reflejen tales condicionantes.
e. En esos supuestos, la Autoridad judicial realiza un doble análisis de la pertinencia y necesidad de la indagación peticionada (arts. 311, 659, 785 y 786.2 LECRIM).

En relación con lo cual cabe apuntar que el contenido del artículo 26, cuando establece que los datos personales figuren en una resolución judicial, o en un registro, diligencias o expedientes tramitados en el curso de investigaciones y procesos penales, hace necesario que el ejercicio de los derechos de las personas interesadas se lleve a cabo de conformidad con las normas procesales penales está entendiendo que en primer lugar se actué conforme a éstas normas y que solo en defecto de regulación en dichas normas a la hora de tratar los datos personales, se aplicará lo dispuesto en la LOPDP.

Imaginemos que una persona interesada solicita a través del ejercicio de del derecho de acceso que se le faciliten los datos de las investigaciones policiales o judiciales (ej.: acceso a las intervenciones telefónicas a la Unidad policial que las efectúa por mandato judicial o el acceso a sus datos de los sistemas de coordinación de investigaciones policiales). Esto obviamente no forma parte de la estructura y contenido del derecho de acceso puesto que el acceso a cada una de las actuaciones se deberá llevar a cabo por la legislación procesal penal o policial aplicable. Si quiere acceder a partes de proceso debe solicitarlo a la autoridad judicial conforme a los derechos que le asisten como tal y será esta la que decida sobre esta cuestión; no teniendo en ningún caso la facultad de acceder por esta vía a tratamientos que amparen actuaciones pre-procesales o procesales que no se deban incorporar a las actuaciones llevadas a cabo por las Fuerzas y Cuerpos de Seguridad competentes.

Veamos un resumen del sistema de restricción de derechos descrito hasta este momento en la siguiente tabla.:

RESOLUCIÓN	ACTUACIÓN	OBJETO MATERIAL	REQUISITOS FORMALES
RESPONSABLE TRATAMIENTO	APLAZAR, LIMITAR U OMITIR DERECHO INFORMACIÓN	Art. 21.2 Derecho de información. a) La base jurídica del tratamiento. b) El plazo durante el cual se conservarán los datos personales o, cuando esto no sea posible, los criterios utilizados para determinar ese plazo. c) Las categorías de destinatarios de los datos personales, cuando corresponda, en particular, los establecidos en Estados que no sean miembros de la Unión Europea u organizaciones internacionales. d) Cualquier otra información necesaria, en especial, cuando los datos personales se hayan recogido sin conocimiento del interesado.	Siempre que, teniendo en cuenta los derechos fundamentales y los intereses legítimos de la persona afectada, resulte necesario y proporcional para la consecución de los siguientes fines: a) Impedir que se obstaculicen indagaciones, investigaciones o procedimientos judiciales. b) Evitar que se cause perjuicio a la prevención, detección, investigación y enjuiciamiento de infracciones penales o a la ejecución de sanciones penales. c) Proteger la seguridad pública. d) Proteger la Seguridad Nacional. e) Proteger los derechos y libertades de otras personas
RESPONSABLE TRATAMIENTO	DENEGAR, TOTAL O PARCIALMENTE DERECHOS	Art. 24.1 El acceso del interesado a sus datos personales, a su rectificación, supresión y la limitación de su tratamiento.	
RESPONSABLE TRATAMIENTO	RESTRICCIÓN DERECHOS	Art. 24.2 El acceso del interesado a sus datos personales, su rectificación, la supresión y la limitación de su tratamiento.	Informará por escrito al interesado sin dilación indebida, y en todo caso, en el plazo de un mes a contar desde que tenga conocimiento, de dicha restricción, **de las razones de la misma**, así como de las posibilidades de presentar una reclamación ante la autoridad de protección de datos, sin perjuicio de las restantes acciones judiciales que pueda ejercer en virtud de lo dispuesto en esta Ley Orgánica. Las razones anteriores de la restricción podrán ser omitidas o ser sustituidas por una redacción neutra cuando la revelación de los motivos de la restricción pueda poner en riesgo los fines a los que se refiere el cuadro superior (apartados a) a e)) El responsable del tratamiento documentará los fundamentos de hecho o de derecho en los que se sustente la decisión denegatoria del ejercicio del derecho de acceso. Dicha información estará a disposición de las autoridades de protección de datos.

RESOLUCIÓN	ACTUACIÓN	OBJETO MATERIAL	REQUISITOS FORMALES
RESPONSABLE TRATAMIENTO	EJERCICIO DERECHOS PROCESOS PENALES: DATOS EN RESOLUCIÓN JUDICIAL, REGISTRO, DILIGENCIAS O EXPEDIENTES TRAMITADOS EN EL CURSO EN EL CURSO INVESTIGACIÓN PENALES	Art. 26. Estos se realizarán conforme a las normas procesales penales, salvo que los responsables sean Jueces o Fiscales que se realizará conforme LOPJ, normas procesales penales y EOMF.	Los responsables policiales darán acceso a dichos datos conforme a lo que disponen las normas procesales penales, sólo acudirán a los artículos anteriores en el caso de que no se regule en la normativa el supuesto sometido a consideración.
AUTORIDAD DE CONTROL	SI SE RESTRINGEN LOS DERECHOS, EL INTERSADO A TRAVES DE LA AUT.CONTROL,	Art.25. La autoridad de control debe informar, al menos, de que se han hecho comprobaciones necesarias, las revisiones que ha hecho y su derecho a ir a contencioso-administrativo.	La autoridad de control no le facilita los datos al interesado, solo informa del resultado de sus actuaciones.

2.2. ¿Derecho específico a la cancelación de antecedentes policiales?

En primer lugar, consideraremos que los denominados antecedentes policiales son datos personales tratados por sus autoridades competentes de conformidad con 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 o cualquier otra disposición legal que complemente o cumpla con dichas finalidades, que se hallen almacenados en un fichero y son obtenidos conforme a bases de legitimación diferentes del consentimiento de la persona afectada.

Estos tratamientos distinguen claramente entre las distintas categorías de interesados (supuestos autores, víctimas, denunciados, testigos, etc.) y su relación con los hechos, salvaguardándose en todos los casos sus derechos y, en particular, garantizándose el derecho a la presunción de inocencia, cuestión ésta que será dirimida por las Autoridades Judiciales o Administrativas competentes.

Estos antecedentes policiales son conformados por hechos tipificados en el vigente Código Penal como infracciones penales o bien aquellos otros hechos de carácter administrativo que han dado lugar por parte de las Fuerzas y Cuerpos de Seguridad del Estado a la instrucción de diligencias y su posterior remisión a las Autoridades Judiciales o Administrativas correspondientes.

Los ciudadanos tendrán sobre dichos tratamientos de datos los derechos regulados en su aspecto material por la LOPDP. El ejercicio de éstos resulta de carácter personalísimo e independiente, de tal forma que la solicitud de uno no es requisito para el otro.

Respecto a este derecho, en la página web del Ministerio del Interior[19] se detallan los aspectos prácticos para su supresión, a saber:

[19] http://www.interior.gob.es/web/servicios-al-ciudadano/cancelacion-de-antecedentes-policiales/procedimiento

- Supresión de oficio: Se tendrán en cuenta los plazos de prescripción de responsabilidad penal establecidos en el Código Penal.
- Supresión a instancia de parte: Se decretará en aquellos casos en que la Autoridad Judicial haya dictado sentencia condenatoria contra el solicitante, siendo preceptiva para llevarse a efecto, la previa supresión de los antecedentes penales derivados de dicha sentencia, en el Registro Central de Penados del Ministerio de Justicia.
- También procederá la supresión: En los casos en los que la resolución adoptada por la Autoridad Judicial sea de absolución, sobreseimiento libre o archivo. Asimismo, se decretará en los casos en que, aun siendo la sentencia judicial condenatoria, hayan transcurrido cinco años, a contar desde la fecha de remisión definitiva de la pena impuesta, sin que se hayan incorporado nuevos datos desfavorables al expediente personal del solicitante.
- Se podrá denegar la solicitud, aun cumplimentados los trámites establecidos en los párrafos anteriores, cuando el certificado de antecedentes penales no sea negativo o esté pendiente de juicio, cuando el solicitante se encuentre cumpliendo el plazo de suspensión de condena impuesta por la Autoridad Judicial o tenga otras responsabilidades pendientes, judiciales o administrativas, cuando tenga antecedentes policiales sin cancelar en alguno de los ficheros de cualquier Fuerza o Cuerpo de Seguridad. En la comunicación al interesado, se hará constar los motivos por los que se le deniega, los recursos y plazos que le asisten según la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas y LOPDP.

Para ejercer los derechos, hay que rellenar u obtener los siguientes documentos:

Instancia de solicitud en la que se hagan constar los datos de filiación completos, el domicilio actual y en el caso de que se pretenda una supresión y/o anulación parcial, el antecedente concreto a que se refiera la solicitud. En el caso de ejercitar en exclusiva el derecho de rectificación, habrá que especificar a qué datos se refiere y la corrección que haya de realizarse, acompañando documentación justificativa de lo solicitado.

Cuando la solicitud de supresión derive de antecedentes por infracciones penales, un certificado de las Autoridades Judiciales correspondientes o copia compulsada del mismo acreditando la firmeza de la resolución y finalización del procedimiento adoptados respecto al antecedente o antecedentes que se desean cancelar y/o anular, o bien no oponerse expresamente a que por parte del Órgano responsable del Tratamiento se recaben dichos datos.

En el caso de sanciones administrativas, certificación del órgano administrativo competente o copia compulsada de la misma que acredite el pago efectivo de la multa o estar exento de responsabilidad por los hechos que motivaron los antecedentes.

En caso de actuar a través de representante legal, poder de representación específico para el ejercicio del derecho correspondiente conforme a lo dispuesto en los 5 y 6 de la Ley 39/2015, de 1 de octubre

Para el ejercicio de los derechos enumerados anteriormente deberá dirigirse a los responsables de tratamiento de las Direcciones Generales de la Policía y de la Guardia Civil, según corresponda.

Además, existe un procedimiento independiente para la supresión de datos personales existentes en el Sistema VioGén (Sistema de Seguimiento Integral de los Casos de Violencia de Género).

En este sentido, debe señalarse que el Sistema VioGén es un tratamiento de datos de carácter personal cuyo responsable es la persona titular de la Dirección General de Coordinación y Estudios del Ministerio de Interior.

Este tratamiento desarrolla las actividades necesarias para garantizar la seguridad y protección de las víctimas de violencia de género, facilitar el seguimiento de las medidas aplicadas y prevenir actividades delictivas vinculadas a la violencia de género con la finalidad de proteger a dichas víctimas y prevenir infracciones penales sobre las mujeres que se puedan ser sujetos pasivos de tales conductas.

Las personas que se consideran interesadas en este fichero serán las víctimas de hechos susceptibles de ser tipificados como violencia de género y las personas incursas en procedimientos e investigaciones judiciales relacionadas con esos mismos hechos, sin que dicha inclusión prejuzgue el derecho a la presunción de inocencia, cuestión ésta que será dirimida por las Autoridades Judiciales competentes.

La información sobre este fichero y toda la relativa a la forma de ejercer los derechos por parte de los interesados se puede obtener en extenso en la página web[20] del Departamento.

Dada la finalidad de este tratamiento y su descripción, en correspondencia con los derechos fundamentales susceptibles de ponderación, en cuanto al ejercicio del derecho de supresión, cabe señalar que los datos registrados en el Sistema VioGén serán conservados de conformidad con el artículo 8 de la LOPDP y sólo serán suprimidos a instancia de las personas interesadas en aquellos casos que exista una resolución judicial firme de sobreseimiento definitivo, una sentencia absolutoria firme y se cancelen los antecedentes penales (judiciales) derivados de las mismas.

Pudiendo, no obstante, ser denegadas aquellas solicitudes de supresión de datos cuando los mismos sigan siendo necesarios para la consecución de los fines para los que fueron recabados (protección a las víctimas y prevención de infracciones penales relacionadas con violencia de género), o cuando haya habido cualquier reiteración, reincidencia o quebrantamiento de las medidas judiciales o las penas. Sin perjuicio de aplicar el artículo 24 de la LOPDP si fuese necesario y estuviera motivado el aplicar alguna restricción a los derechos de información, acceso, rectificación, supresión de datos personales y a la limitación de su tratamiento.

En relación con lo señalado resulta ineludible aportar la documentación compulsada que acredite la firmeza de las resoluciones y la finalización de los procedimientos (sentencia absolutoria, archivo, sobreseimiento o ejecutoria de cumplimiento de condena (para estos casos requiere la acreditación previa de cancelación de antecedente penal)

[20] http://www.interior.gob.es/web/servicios-al-ciudadano/participacion-ciudadana/proteccion-de-datos-de-caracter-personal/tutela-de-los-derechos#normativa

Los formularios podrán presentarse, para validación y registro preceptivo, ante cualquier dependencia de Policía Nacional o Guardia Civil, así como ante cualquier oficina de las Delegaciones o Subdelegaciones del Gobierno, existentes en cada provincia, a través del Registro Electrónico General de la Administración General del Estado de acuerdo a lo dispuesto en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas)

Las solicitudes se responderán en el plazo de un mes, aunque, si se tiene en cuenta la complejidad y número de solicitudes, se podría prorrogar el plazo otros dos meses más (lo cual será trasladado al interesado).

III. OTRAS CUESTIONES DE INTERÉS

1. Derecho a recibir notificaciones de las brechas de seguridad

Para el estudio de esta cuestión nos basaremos en la Guía para la notificación de brechas de datos personales que ha elaborado la AEPD en su versión de junio de 2021.

En primer lugar, señalaremos que la finalidad última de la notificación y comunicación de brechas de datos personales es la protección efectiva de los derechos fundamentales y libertades de las personas físicas afectadas por la brecha.

Este derecho se deriva de las obligaciones recogidas en los artículos 33 y 34 del RGPD y 38 y 39 de la LOPDP, 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, tanto a nivel nacional, como con relación a los criterios establecidos por el Comité Europeo de Protección de Datos (CEPD) y la Agencia Española de Protección de Datos (AEPD)

Las entidades que sufran una brecha de datos personales deben focalizar sus esfuerzos en evitar y mitigar las posibles consecuencias sobre los derechos fundamentales y libertades públicas de las personas afectadas.

Debemos puntualizar que no todos los incidentes de seguridad son necesariamente brechas de datos personales y no solo los ciberincidentes pueden ser brechas de datos personales. A su vez, no toda acción que suponga una vulneración de la normativa de protección de datos puede ser considerada una brecha de datos personales. Y es que no tendrán la consideración de brecha de datos personales aquellos incidentes que:

- No afecten a datos personales, es decir, a datos que no sean de personas físicas identificadas o identificables.
- No afecten a tratamientos de datos personales llevados a cabo por un responsable o un encargado.
- Ocurran en tratamientos llevados a cabo por una persona física en el ámbito doméstico.

El RGPD adopta una definición de carácter amplio al señalar como brechas de datos personales *«todas aquellas violaciones de la seguridad que ocasionen la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos»*.

En caso de detectarse una brecha de datos personales en la organización, y a efectos de una correcta y eficaz gestión, será necesaria la colaboración y actuación de distintas figuras. Para que cada una de las personas implicadas pueda actuar de forma efectiva, previamente deben haberse establecidos los procedimientos y articulado los medios necesarios.

Conforme al artículo 33 del RGPD y 38 de la LOPDP, tan pronto como el responsable del tratamiento tenga conocimiento de que se ha producido una brecha de datos personales debe efectuar la correspondiente notificación a la Autoridad de Control competente, cuando sea probable que la brecha constituya un riesgo

para los derechos y libertades de las personas. En su caso, debe realizarse sin dilación y a más tardar en las 72 horas siguientes, computando también las horas trascurridas durante fines de semana y festivos.

No obstante, si el responsable puede garantizar que es improbable que la brecha de datos personales entrañe un riesgo para los derechos y las libertades de las personas físicas no habrá obligación de notificarlo.

Si la brecha de datos personales es detectada por el encargado del tratamiento éste deberá remitir al responsable toda la información necesaria para que pueda cumplir con sus obligaciones en tiempo y forma. El responsable debe documentar la brecha y evaluar tanto la necesidad de notificar ante la Autoridad de Control como la necesidad de comunicar a los afectados. El encargado podrá realizar la notificación de brecha de datos personales en nombre de los responsables involucrados cuando así lo tengan estipulado en un contrato o vínculo legal.

Cuando la brecha de datos personales entrañe un alto riesgo para los derechos y libertades de las personas afectadas, además de la notificación a la Autoridad de Control, se deberá comunicar a los afectados la brecha de datos personales sin dilación indebida, salvo en algunos supuestos, expuestos y determinados en la guía de referencia. El lenguaje será claro y sencillo, de forma concisa y transparente.

La notificación de brechas de datos personales a la Autoridad de Control deberá como mínimo:

- Describir la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados;
- Comunicar el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto del que pueda obtenerse más información;
- Describir las posibles consecuencias de la violación de la seguridad de los datos personales;
- Describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

A continuación, se plasman en un cuadro las funciones y responsabilidades de los diferentes roles en estos casos[21]:

Figura	Funciones y responsabilidades
Responsable	• Implantación del proceso de gestión de brechas • Evaluación de las consecuencias para los derechos y libertades de las personas • Notificar la brecha de datos personales a la Autoridad de Control • Comunicar la brecha de datos personales a las personas afectadas

[21] «Guía para la notificación de brechas de datos personales» AEPD, v. 2021.

Figura	Funciones y responsabilidades
Encargado	• Informar al responsable de las brechas de datos personales que afecten a los tratamientos encargados • Ayudar al responsable en la gestión de la brecha de datos personales • Ejecutar las labores de notificación o comunicación de la brecha que tenga asignadas por contrato
Delegado de protección de datos	• Informar y asesorar al responsable/encargado del tratamiento sobre sus obligaciones y responsabilidades con relación a las brechas de datos personales • Cooperar con la Autoridad de Control en las cuestiones relativas a la gestión de la brecha de datos personales • Actuar como punto de contacto con la Autoridad de Control, en particular, en el proceso de notificación de la brecha de datos personales

Los interesados afectados serán las personas físicas cuyos datos personales se han visto afectados por una brecha comprometiendo la confidencialidad, integridad y/o disponibilidad de esos datos, y quienes pueden sufrir las consecuencias.

En todo caso, el proceso de gestión de brechas de datos personales establecido en la organización deberá incluir un procedimiento para llevar a cabo la comunicación de la brecha de datos personales a los interesados afectados, concretando la información contenida en los siguientes apartados, inclusive estableciendo los plazos concretos adecuados.

Se establece que cuando sea probable que la brecha de datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable de tratamiento comunicará la brecha de datos personales a los afectados sin dilación indebida.

No será necesaria la comunicación a los afectados cuando:

- El responsable ha tomado medidas técnicas y organizativas adecuadas que evitan los riesgos anteriores, minimizan los daños a los derechos y libertades y/o los hacen reversibles.
- El responsable ha tomado con posterioridad a la brecha de datos personales las medidas de protección que mitiguen total o parcialmente el posible impacto para los afectados y garanticen que ya no hay posibilidad de que el alto riesgo para sus derechos y libertades se materialice.

La comunicación de una brecha de datos personales a las personas afectadas conforme corresponde al responsable del tratamiento el cual lo realizará a través del cauce que considere oportuno, por ejemplo, a través del Delegado de Protección de Datos si lo tiene designado.

Esta comunicación a las personas afectadas se realizará en un lenguaje claro y sencillo, conteniendo al menos los datos de contacto del Delegado de Protección de Datos, o en su caso, del punto de contacto en el que pueda obtenerse más in-

formación, la descripción general del incidente y momento en que se ha producido, las posibles consecuencias de la brecha de datos personales, la descripción de los datos e información personal afectados, el resumen de las medidas implantadas hasta el momento para controlar los posibles daños y cualquier otra reseña útil a los afectados para que puedan proteger sus datos o prevenir posibles daños.

Nos señala la AEPD que la comunicación preferentemente se deberá realizar de forma directa al afectado, ya sea por teléfono, correo electrónico, SMS, a través de correo postal, o a través de cualquier otro medio dirigido al afectado que el responsable considere adecuado.

Sin perder de vista que una comunicación incompleta (sin el contenido mínimo), de difícil acceso o realizada a las personas incorrectas no es efectiva, por lo que una comunicación en estas condiciones podría llegar a considerarse una comunicación no realizada con las correspondientes consecuencias derivadas de tal actuación.

Del mismo modo, en este apartado, sería importante que el responsable tuviera presente un elemento de consulta fundamental como son las Directrices 01/2021 del CEPD sobre ejemplos relacionados con la notificación de violación de datos personales (Versión 14 diciembre 2021)

2. Derechos digitales

La LOPDGDD regula en su Título X (artículos 79 a 97) la garantía de los derechos digitales, con el fin de establecer un reconocimiento de un sistema de garantía de los derechos digitales de la ciudadanía para hacer posible el pleno ejercicio de los derechos fundamentales en la realidad digital.

En lo que concierne a los derechos de los ciudadanos en este ámbito, debemos señalar como derechos, el acceso universal a Internet, el derecho a la seguridad digital, el derecho a la educación digital, el derecho de rectificación en Internet, derecho a la actualización de informaciones en medios de comunicación digitales, derecho al olvido, derecho de portabilidad, derecho al testamento digital.

En el ámbito laboral, nos encontramos con el derecho a la intimidad y uso de dispositivos digitales, derecho a la desconexión digital y el derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo.

Veamos a continuación de manera sucinta en qué consisten estos derechos *«básicos»*:

- Acceso universal a Internet- este derecho comprende la garantía a un acceso asequible, de calidad y no discriminatorio para toda la población.
- Seguridad digital- los proveedores de servicios de Internet informarán a los usuarios de sus derechos.
- Educación digital- El sistema educativo garantizará la plena inserción del alumnado en la sociedad digital y el aprendizaje de un uso de los medios digitales que sea seguro y respetuoso con la dignidad humana, los valores constitucionales, los derechos fundamentales y, particularmente con el respeto y la garantía de la intimidad personal y familiar y la protección de datos personales

- Rectificación en Internet- implica el derecho a la libertad de expresión en Internet. Los responsables de redes sociales y servicios equivalentes adoptarán protocolos adecuados para posibilitar el ejercicio del derecho de rectificación ante los usuarios que difundan contenidos que atenten contra el derecho al honor, la intimidad personal y familiar en Internet y el derecho a comunicar o recibir libremente información veraz
- Actualización de informaciones en medios de comunicación digitales- derecho a solicitar motivadamente de los medios de comunicación digitales la inclusión de un aviso de actualización suficientemente visible junto a las noticias que le conciernan cuando la información contenida en la noticia original no refleje su situación actual como consecuencia de circunstancias que hubieran tenido lugar después de la publicación, causándole un perjuicio.
- Derecho al olvido en búsquedas de Internet- derecho a que los motores de búsqueda en Internet eliminen de las listas de resultados que se obtuvieran tras una búsqueda efectuada a partir de su nombre los enlaces publicados que contuvieran información relativa a esa persona cuando fuesen inadecuados, inexactos, no pertinentes, no actualizados o excesivos o hubieren devenido como tales por el transcurso del tiempo, teniendo en cuenta los fines para los que se recogieron o trataron, el tiempo transcurrido y la naturaleza e interés público de la información.
- Derecho al olvido en servicios de redes sociales y servicios equivalentes- derecho a que sean suprimidos, a su simple solicitud, los datos personales que hubiese facilitado para su publicación por servicios de redes sociales y servicios de la sociedad de la información equivalentes
- Portabilidad en servicios de redes sociales y servicios equivalentes - derecho a recibir y transmitir los contenidos que hubieran facilitado a los prestadores de dichos servicios, así como a que los prestadores los transmitan directamente a otro prestador designado por el usuario, siempre que sea técnicamente posible.
- Testamento digital- reglas respecto al acceso de contenidos gestionados por prestadores de servicios de la sociedad de la información sobre personas fallecidas.

En cuanto a los derechos digitales en el ámbito laboral, podemos resumirlos de la siguiente forma:

- Derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral. El empleador podrá acceder a los contenidos derivados del uso de medios digitales facilitados a los trabajadores a los solos efectos de controlar el cumplimiento de las obligaciones laborales o estatutarias y de garantizar la integridad de dichos dispositivos.
  Los empleadores deberán establecer criterios de utilización de los dispositivos digitales respetando en todo caso los estándares mínimos de protección de su intimidad de acuerdo con los usos sociales y los derechos reconocidos constitucional y legalmente. En su elaboración deberán participar los representantes de los trabajadores.

El acceso por el empleador al contenido de dispositivos digitales respecto de los que haya admitido su uso con fines privados requerirá que se especifiquen de modo preciso los usos autorizados y se establezcan garantías para preservar la intimidad de los trabajadores, tales como, en su caso, la determinación de los períodos en que los dispositivos podrán utilizarse para fines privados.

Los trabajadores deberán ser informados de los criterios de utilización a los que se refiere este apartado

- Derecho a la desconexión digital en el ámbito laboral. Los trabajadores y los empleados públicos tendrán derecho a la desconexión digital a fin de garantizar, fuera del tiempo de trabajo legal o convencionalmente establecido, el respeto de su tiempo de descanso, permisos y vacaciones, así como de su intimidad personal y familiar

  Las modalidades de ejercicio de este derecho atenderán a la naturaleza y objeto de la relación laboral, potenciarán el derecho a la conciliación de la actividad laboral y la vida personal y familiar y se sujetarán a lo establecido en la negociación colectiva o, en su defecto, a lo acordado entre la empresa y los representantes de los trabajadores.
- Derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo. Los empleadores podrán tratar las imágenes obtenidas a través de sistemas de cámaras o videocámaras para el ejercicio de las funciones de control de los trabajadores o los empleados públicos previstas, respectivamente, en el artículo 20.3 del Estatuto de los Trabajadores y en la legislación de función pública, siempre que estas funciones se ejerzan dentro de su marco legal y con los límites inherentes al mismo. Los empleadores habrán de informar con carácter previo, y de forma expresa, clara y concisa, a los trabajadores o los empleados públicos y, en su caso, a sus representantes, acerca de esta medida.

  En el supuesto de que se haya captado la comisión flagrante de un acto ilícito por los trabajadores o los empleados públicos se entenderá cumplido el deber de informar cuando existiese al menos el dispositivo al que se refiere el artículo 22.4 de esta ley orgánica.

  En ningún caso se admitirá la instalación de sistemas de grabación de sonidos ni de videovigilancia en lugares destinados al descanso o esparcimiento de los trabajadores o los empleados públicos, tales como vestuarios, aseos, comedores y análogos

  La utilización de sistemas similares a los referidos en los apartados anteriores para la grabación de sonidos en el lugar de trabajo se admitirá únicamente cuando resulten relevantes los riesgos para la seguridad de las instalaciones, bienes y personas derivados de la actividad que se desarrolle en el centro de trabajo y siempre respetando el principio de proporcionalidad, el de intervención mínima y las garantías previstas en los apartados anteriores. La supresión de los sonidos conservados por estos sistemas de grabación se realizará atendiendo a lo dispuesto en el apartado 3 del artículo 22 de esta ley
- Derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral. Los empleadores podrán tratar los datos obtenidos a

través de sistemas de geolocalización para el ejercicio de las funciones de control de los trabajadores o los empleados públicos previstas, respectivamente, en el artículo 20.3 del Estatuto de los Trabajadores y en la legislación de función pública, siempre que estas funciones se ejerzan dentro de su marco legal y con los límites inherentes al mismo

Con carácter previo, los empleadores habrán de informar de forma expresa, clara e inequívoca a los trabajadores o los empleados públicos y, en su caso, a sus representantes, acerca de la existencia y características de estos dispositivos. Igualmente deberán informarles acerca del posible ejercicio de los derechos de acceso, rectificación, limitación del tratamiento y supresión.

3. Protocolo General de Actuación entre el Ministerio del Interior y la Agencia Española de Protección de Datos para la colaboración en materia de atención a las personas afectadas en caso de que sus datos se hayan obtenido ilegítimamente y difundido a través de internet, especialmente en caso de imágenes, vídeos o audios con datos sensibles

Esta herramienta fue firmada el 24 de septiembre de 2019, siendo el cauce de colaboración mediante el que las partes firmantes instrumentalizaban como realizar varias actuaciones entre las que se encuentran, entre otras, las siguientes:

- Cuando se presente denuncia ante la Policía o ante la Guardia Civil, si a raíz de los hechos que se declarasen, se detectasen indicios de conductas que vulneran la legislación en materia de protección de datos, se informará a la persona denunciante acerca de su derecho a presentar una reclamación ante la AEPD. Se informará, asimismo, de que la reclamación que se pueda presentar ante la Agencia es gratuita.
- Analizar en todo caso las medidas necesarias para informar a las Fuerzas y Cuerpos de Seguridad de cómo proceder para la presentación de reclamaciones ante la AEPD y obtener evidencias que faciliten la actuación de la AEPD, en aquellos casos en los que la reclamación se presente directamente por aquéllas.
- La AEPD informará al MIR acerca de los materiales didácticos -dirigidos a las distintas etapas y niveles educativos- que se desarrollen, bien directamente por la propia Agencia, bien en el contexto de la colaboración con el Ministerio de Educación, Cultura y Deporte. De este modo, los miembros de las Fuerzas y Cuerpos de Seguridad que realicen acciones de formación y difusión en centros educativos, podrán conocer estos materiales y proporcionar su referencia a la comunidad educativa.
- La AEPD colaborará en los programas de formación para empleados del MIR en materia de protección de datos, singularmente en aquéllos que se dirijan específicamente a miembros de las Fuerzas y Cuerpos de Seguridad.
- Por su parte, el MIR colaborará en las acciones formativas que se desarrollen relativas a la concienciación, prevención, detección o investigación de conductas de violencia sobre la mujer.

Por parte del Ministerio del Interior se efectuaron las correspondientes ampliaciones para que el interesado conociese estas posibilidades en el contenido de los *«Formularios de información de derechos a víctima o perjudicado»* que confeccionen los dos Cuerpos policiales estatales, cuyo contenido fue tratado, discutido y ratificado en la reunión de la Comisión Nacional de Coordinación de Policía Judicial de 4 de junio de 2021.

Desde ese momento, la información de derechos que se entregue a las personas denunciantes en los ilícitos penales que lo hagan oportuno incluiría una previsión similar a.

> *«Para hacer efectivos los derechos a la protección de sus datos de carácter personal, tiene derecho a presentar una reclamación gratuita ante la Agencia Española de Protección de Datos (AEPD), y cuando los datos se hayan obtenido o se difundan ilegítimamente o constituyan datos especialmente sensibles (de carácter sexual o violento), puede utilizar el canal prioritario de la AEPD para comunicar y solicitar su retirada y preservación para la investigación penal.*
>
> *Puede hacerlo efectivo en el enlace disponible en la página web de la AEPD: https://www.aepd.es/canalprioritario/»*

Este Canal Prioritario[22] es una herramienta que se puede utilizar si tiene conocimiento de que están alojadas en páginas o repositorios en Internet imágenes de contenido sexual o que muestran actos de agresión, cuya difusión sin el consentimiento de las personas afectadas ponga en alto riesgo sus derechos y libertades, y que no se haya logrado su retirada a través de los canales especialmente previstos por el prestador de servicios.

Al utilizar dicho procedimiento, el interesado deberá describir detalladamente las circunstancias en que se ha producido la difusión no consentida de las imágenes, indicando en particular si la persona afectada es víctima de violencia de género, abuso o agresión sexual o acoso y si pertenece a cualquier otro colectivo especialmente vulnerable.

La herramienta nos demanda que copiemos y peguemos la dirección o direcciones web de acceso o identifique claramente el perfil social a través del que se están difundiendo, se especifique si ha llevado a cabo acciones para denunciar los hechos ante las instancias policiales, detallando, en tal caso, las instancias administrativas o judiciales concretas y la referencia de los procedimientos que se estén tramitando y si se han llevado a cabo acciones para limitar la difusión de los datos personales, identificando claramente, en tal caso, a los prestadores de servicios a los que se ha dirigido la persona.

Del mismo modo, solicita que se incorporen a la petición los documentos que se consideren relevantes para la tramitación de su reclamación, particularmente una copia de la pantalla o del dispositivo donde pueda apreciarse claramente el servicio (la red social, el portal de vídeo o de blogs ...) a través del cual se están difundiendo las imágenes.

---

[22] https://sedeagpd.gob.es/sede-electronica-web/vistas/formNuevaReclamacion/nuevaReclamacion.jsf?QID=Q600&ce=0

Tras el análisis de la reclamación y los documentos que la acompañan, la AEPD determinará la posible adopción de las medidas urgentes a las que le habilita el RGPD y la LOPDGDD que limitarán la continuidad del tratamiento de los datos personales por parte de los distintos responsables del tratamiento.

CAPÍTULO 4
TRATAMIENTO DE DATOS PERSONALES EN EL ÁMBITO DE LA VIDEOVIGILANCIA POR LAS FUERZAS Y CUERPOS DE SEGURIDAD

I. ANTECEDENTES Y SITUACIÓN

La Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos, ya en el año de su publicación recogía en su parte expositiva que:

> *«La prevención de actos delictivos, la protección de las personas y la conservación y custodia de bienes que se encuentren en situación de peligro, y especialmente cuando las actuaciones perseguidas suceden en espacios abiertos al público, lleva a los miembros de las Fuerzas y Cuerpos de Seguridad al empleo de medios técnicos cada vez más sofisticados. Con estos medios, y en particular mediante el uso de sistemas de grabación de imágenes y sonidos y su posterior tratamiento, se incrementa sustancialmente el nivel de protección de los bienes y libertades de las personas.»*

Como puede observarse el legislador entendía que se utilizaban medios tecnológicos cada vez más potentes y con mayor grado de autonomía. Pero si nos detenemos a analizar los dispositivos de toma de imágenes de ese año podemos observar que la cámara fotográfica que ocupaba el 40 % de la cuota de mercado estadounidense estaba dotada de disquete de memoria (no tarjeta), tenía un zoom óptico de 10 aumentos y estaba equipada con un sensor de 0,3 megapíxeles. Las videocámaras comenzaron el año anterior, 1996, a desarrollarse con el formato digital (DV) y fue entre los años 1999 y 2000 cuando se desarrollaron los teléfonos móviles con cámaras (el modelo Samsung SHC-V200 (años 2000), podía registrar 20 imágenes de 0,35 megapíxeles, y verse en una pantalla de 1,5 pulgadas y el Sharp J-SH04, podía registrar imágenes de 0,11 megapíxeles y enviarlas utilizando la conectividad del teléfono[1]).

[1] https://www.xataka.com/moviles/el-comienzo-de-la-comunicacion-visual-instantanea-la-camara-y-el-movil-se-conocieron-en-un-parto-en-1997

En el año 2021, una cámara de fotografía o video (o ambos sistemas) profesional tiene características estándar de unos 20-24 megapíxeles, grabación en 4k, full HD, entrada de micrófono, zoom, estabilizadores, sistemas de almacenamiento internos y externos con capacidades de Gigabytes, etc. Por su parte, un Smartphone de gama alta tiene varias cámaras de video-audio con características próximas a 100 MP f/1.8, Ultra gran angular 12 MP f/2.2, Tele 10 MP f/2.4, Tele 10 MP f/4.9 y Láser AF ToF, etc...

Estos datos muestran un panorama que ha evolucionado exponencialmente en apenas dos décadas y que proporciona unas posibilidades inimaginables.

Todo ello sin sumar las posibilidades de tratamientos de las imágenes captadas a través de sistemas térmicos o termográficos, de reconocimiento biométrico o del empleo de programas de inteligencia artificial.

Al igual que ocurre en todos los campos sociales, como no puede ser de otra manera, cada vez resulta más frecuente la utilización de sistemas grabación y videovigilancia[2] por parte de las FCS, captando a través de ellos imágenes y, en ocasiones, la propia voz de los ciudadanos, siendo importante, por lo tanto, el conocer en profundidad el marco normativo aplicable al tratarse de mecanismos que inciden directamente en la esfera de los derechos fundamentales de las personas.

En concreto, como hemos analizado previamente en este libro, se ven afectados de manera especial el derecho a la protección de datos, al honor, a la intimidad y a la propia imagen, y otros derechos que inciden directamente en la esfera de privacidad de los individuos. Como regla general, la captación de imágenes y sonidos, con fines de seguridad de la vía pública será realizada por las FCS, amparados en los supuestos regulados que se irán analizando. Cabe señalar que no se podrán utilizar videocámaras para tomar imágenes y sonidos del interior de viviendas, ni de sus vestíbulos, salvo consentimiento del titular o autorización judicial, ni de los lugares públicos abiertos o cerrados cuando se afecte de forma directa y grave a la intimidad de las personas, así como tampoco para grabar conversaciones de naturaleza estrictamente privada, salvo en los supuestos amparados por la ley y con las garantías necesarias para realizar tales actuaciones.

El derecho a la imagen está reconocido por el artículo 18.1 CE, y junto al honor y a la intimidad personal y familiar, se integra en los derechos de la personalidad. El Tribunal Constitucional ha señalado que el derecho a la propia imagen derivado de este artículo se configura como un derecho de la personalidad que refuerza la dignidad humana y se sitúa en la esfera moral de la persona. Como sucede con el resto de derechos, el de la propia imagen, tampoco es absoluto, encontrando límites en otros derechos y bienes constitucionalmente protegidos.

Un dato personal requiere que concurran, por un lado, la existencia de una información y, por otro, que esta pueda vincularse a una persona física identificada o identificable, conforme se deriva de lo dispuesto en el artículo 4.1 del RGPD y en el artículo 5 de la LOPDP.

En definitiva, la imagen de una persona en la medida que identifique o pueda identificar a la misma constituye un dato de carácter personal objeto de tratamien-

[2] Real Academia Española. Videovigilancia: 1. f. *Vigilancia por medio de un sistema de cámaras, fijas o móviles.*

to, por lo debe ajustarse a los principios y obligaciones que establece la normativa de protección de datos.

La Sentencia del TJUE en el asunto C-212/13, František Ryneš contra Úřad pro ochranu osobních údajů[3], en el que el Reino de España participo como parte interesada, introducía una interesante conclusión sobre este aspecto al entender que:

> *«La videovigilancia que implique la grabación y la conservación de datos personales es objeto de la Directiva de Protección de Datos, ya que constituye el tratamiento automatizado de datos.»*

Desde la publicación de la LOV y el Reglamento de desarrollo y ejecución de la Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos se da cobertura a los derechos y libertades constitucionales que puedan ser vulnerados mediante la utilización de sistemas de videovigilancia, por un lado, el derecho al honor, a la intimidad personal y familiar y a la propia imagen (artículo 2.1 de la LOV) y al tratamiento de datos de carácter personal (artículo 2.2 de la LOV), dando cumplimiento al mandato constitucional recogido en el Artículo 104. 1 de la CE:

> *«Las Fuerzas y Cuerpos de Seguridad, bajo la dependencia del Gobierno, tendrán como misión proteger el libre ejercicio de los derechos y libertades y garantizar la seguridad ciudadana».*

En concreto la LOV, en su artículo 2.1 recoge que *«la captación, reproducción y tratamiento de imágenes y sonidos, en los términos previstos en esta Ley; así como las actividades preparatorias, no se considerarán intromisiones ilegítimas en el derecho al honor, a la intimidad personal y familiar y a la propia imagen, a los efectos de lo establecido en el artículo 2.2 de la Ley Orgánica 1/1982, de mayo»*. Esta misma referencia es recogida en el artículo 15.1 de la LOPDP.

Así, con los presupuestos legales correspondientes, en la prevención de actos delictivos, la protección de las personas y la conservación y custodia de bienes que se encuentren en situación de peligro, especialmente en lugares abiertos al público, las FCS tienen que emplear cada vez medios técnicos más sofisticados. Con estos medios, entre los que se encuentra el uso de sistemas de grabación de imágenes y sonidos se incrementa la seguridad y el nivel de protección de los bienes y libertades de las personas. Pero esta seguridad pretendida a través de la utilización de la videovigilancia requiere de un conjunto de garantías para que el ejercicio de los derechos y libertades constitucionales sea máximo, y no sea perturbado por un exceso de celo en defensa de la seguridad pública.

Este sistema de garantías se estructura a través de un armazón normativo e Instrucciones en materia de videovigilancia que se compone principalmente por:

- CEDH, artículo 8.
- Convenio 108 +, al establecer que las actividades de videovigilancia que impliquen el tratamiento de datos personales serán objeto del ámbito de aplicación del mismo.

[3] https://eur-lex.europa.eu/legal-content/es/TXT/?uri=CELEX:62013CJ0212

- Carta de la UE, artículos 7 y 8.
- Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal.
- 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 (LOPDP).
- 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 (RGPD).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).
- Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos (LOV).
- El Reglamento de desarrollo y ejecución Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos (Reglamento LOV).
- Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana (LOPSC).
- Ley 5/2014, de 4 de abril, de Seguridad Privada (LSP).
- Del mismo modo, en los supuestos en los que los miembros de las FCSE realicen labores en misiones internacionales o cuando la Guardia Civil realice labores militares incardinada en las Fuerzas Armadas tanto en territorio nacional como en zona de operaciones, habrá que atenerse al instrumento normativo que regule tales actuaciones y/o a la normativa del territorio donde se efectúen dichas misiones.

Siendo asimismo muy relevante acudir a la interpretación que se hace de algunos aspectos relacionados con esta materia tanto en la Circular 4/2019, de 6 de marzo, de la Fiscal General del Estado[4], sobre utilización de dispositivos técnicos de captación de la imagen, de seguimiento y de localización como en la *«Guía sobre el uso de videocámaras para seguridad y otras finalidades»* de la AEPD[5], las *«Directrices 3/2019 sobre el tratamiento de datos personales mediante dispositivos de vídeo»* del Comité Europeo de Protección de Datos[6] y la Guía *«Protección de Datos y Administración Local- Guías Sectoriales AEPD»*[7]

En estas últimas directrices, como elemento aclaratorio, se reitera que el tratamiento de datos personales por las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluidas la protección y la prevención frente

[4] https://www.boe.es/diario_boe/txt.php?id=BOE-A-2019-4243

[5] https://www.aepd.es/es/documento/guia-videovigilancia.pdf

[6] https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_es.pdf

[7] https://www.aepd.es/sites/default/files/2019-09/guia-proteccion-datos-administracion-local.pdf

a las amenazas contra la seguridad pública, pertenece al ámbito de aplicación de la DDP y por ende de la LOPDP. Con una particularidad que pensamos derivaría de la falta de claridad de la AEPD con respecto a las funciones de los Cuerpos de Policía Local, puesto que en la última Guía remite todos sus posibles tratamientos a la LOV[8] obviando posibles funciones de prevención, detección o investigación de determinadas infracciones penales por éstos. De esta postura, por supuesto, se difiere amable pero firmemente y se argumentará el parecer de los autores en los apartados siguientes.

Tampoco se puede obviar el contenido de la Recomendación CM / Rec (2017) 6[9], del Comité de Ministros a los Estados miembros del Consejo de Europa sobre *«técnicas especiales de investigación»*, en relación con delitos graves, incluidos actos de terrorismo (Adoptada por el Comité de Ministros el 5 de julio), que aun no siendo vinculante, se recoge de manera interesante el concepto *«Técnicas especiales de investigación»* definiéndolas como aquellas aplicadas por las autoridades competentes en el contexto de investigaciones penales con el fin de prevenir, detectar, investigar, enjuiciar y reprimir delitos graves, con el objetivo de recopilar información de tal manera que no alertar a las personas objetivo, que como vemos, se podría aplicar al uso de dispositivos de grabación de imágenes y sonido.

Esta recomendación marca como condiciones de uso para estas técnicas que sólo deberían utilizarse cuando haya motivos suficientes para creer que una o más personas en particular o un individuo o grupo de individuos aún no identificados han cometido o preparado, o están preparando un delito grave.

Estas cuestiones están recogidas mayoritariamente en nuestra legislación interna, con las particularidades oportunas conforme a nuestro régimen constitucional.

En este capítulo se pretende analizar en profundidad las principales normas en relación con el uso de dispositivos de videovigilancia por las FCS, con el objetivo de aclarar en lo posible las disposiciones aplicables dependiendo del tipo de tratamiento y los requisitos exigidos para el uso de los diferentes tipos de dispo-

---

[8] La Guía determina en su página 45 que: *«¿Se pueden instalar cámaras de videovigilancia que graben la vía pública? La instalación de videocámaras en lugares públicos, tanto fijas como móviles, es competencia exclusiva de las Fuerzas y Cuerpos de Seguridad, rigiéndose el tratamiento de dicha imágenes por su legislación específica, contenida en la Ley Orgánica 4/1997, de 4 de agosto, y su Reglamento de desarrollo, sin perjuicio de que les sea aplicable, en su caso, lo previsto por el RGPD , en aspectos como la adopción de las medidas de seguridad que resulten de aplicación y la elaboración del registro de actividades en relación con el tratamiento de videovigilancia que se realice. Su utilización en lugares públicos tiene una finalidad específica de seguridad en beneficio de la convivencia ciudadana, la erradicación de la violencia y la utilización pacífica de las vías y espacios públicos, así como de prevenir la comisión de delitos, faltas e infracciones relacionados con la seguridad pública. La instalación de este tipo de dispositivos de las imágenes grabadas, están sujetas a requisitos muy estrictos ya que, en primer lugar, la autorización de instalación de videocámaras fijas y la utilización de cámaras móviles se otorga por la Delegación del Gobierno previo informe preceptivo y vinculante de la Comisión de Garantías de la Videovigilancia de la Comunidad Autónoma correspondiente.», y en su página 46: «¿Puede utilizar la policía local cámaras móviles o incluso realizar grabaciones con sus propias cámaras? Aunque se tratase de cámaras móviles o sus propias cámaras, se trataría de un supuesto cuya respuesta es la misma que en la anterior pregunta-respuesta, es decir, aplicación de la Ley Orgánica 4/1997, de 4 de agosto, y su Reglamento de desarrollo, sin perjuicio de que les sea aplicable, en su caso, lo previsto en el RGPD.»*

[9] https://rm.coe.int/1680730408

sitivos de videovigilancia para que dicha actuación sea conforme a la legalidad y respete los derechos fundamentales de las personas afectadas de manera que se cuente siempre con un fundamento jurídico válido que le otorgue el correspondiente soporte.

II. FINALIDAD Y PRINCIPIOS RECTORES DEL USO DE VIDEOCÁMARAS POR LAS FUERZAS Y CUERPOS DE SEGURIDAD

En correspondencia con ese primer mandato, y el sistema implementado por el Derecho de la Unión Europea, la instalación y uso de videocámaras en lugares públicos, tanto fijas como móviles, competencia de las FCS, queda sujeta al tratamiento recogido en la legislación específica contenida en la Ley Orgánica 7/2021, y en todo lo que no la contradigan o se oponga[10], en la LOV y el Reglamento LOV.

Como primera idea básica y general es que se ha pasado de un sistema de autorización o declaración previa de los tratamientos de datos personales a un sistema de «responsabilidad proactiva» de las entidades y personas que realizan estas actuaciones.

Para la aplicación de la LOPDP, es importante tener presente su ámbito de aplicación, así como la definición de autoridad competente:

> *«Artículo 2. Ámbito de aplicación.*
>
> *1. Será de aplicación 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, realizado por las autoridades competentes, con fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, incluidas la protección y prevención frente a las amenazas contra la seguridad pública...»*
>
> *«Artículo 4. Autoridades competentes.*
>
> *1. Será autoridad competente, a los efectos de esta Ley Orgánica, toda autoridad pública que tenga competencias encomendadas legalmente para el tratamiento de datos personales con alguno de los fines previstos en el artículo 1.*
>
> *En particular, tendrán esa consideración, en el ámbito de sus respectivas competencias, las siguientes autoridades:*
>
> *a) Las Fuerzas y Cuerpos de Seguridad.*
>
> *b) Las Administraciones Penitenciarias.*
>
> *c) La Dirección Adjunta de Vigilancia Aduanera de la Agencia Estatal de Administración Tributaria.*
>
> *d) El Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias.*
>
> *e) La Comisión de Vigilancia de Actividades de Financiación del Terrorismo.*
>
> 2. También tendrán consideración de autoridades competentes las Autoridades judiciales del orden jurisdiccional penal y el Ministerio Fiscal.»

La instalación de videocámaras en lugares públicos, tanto fijas como móviles, competencia de las FCS, como autoridad competente en virtud del aludido artículo 4, se adecuará a los dispuesto en la misma, siempre que el tratamiento se enmarque en las finalidades recogidas en el ámbito de aplicación.

---

[10] La disposición derogatoria única de la Ley 7/2021 recoge que *«Quedan derogadas todas las normas de igual o inferior rango en lo que contradigan o se opongan a lo dispuestos en esta Ley Orgánica»*.

En cuanto a la finalidad de los sistemas de grabación de imágenes y sonido por las FCS destaca el Artículo 15.2 de la LOPDP:

> *«2. En la instalación de sistemas de grabación de imágenes y sonidos se tendrán en cuenta, conforme al principio de proporcionalidad, los siguientes criterios: asegurar la protección de los edificios e instalaciones propias; asegurar la protección de edificios e instalaciones públicas y de sus accesos que estén bajo custodia; salvaguardar y proteger las instalaciones útiles para la seguridad nacional y prevenir, detectar o investigar la comisión de infracciones penales y la protección y prevención frente a las amenazas contra la seguridad pública»*

TRATAMIENTO (GRABACIÓN) = AUTORIDAD COMPETENTE + FINES ARTÍCULO 1 LOPDP

La LOV regularía por lo tanto las competencias de las FCS para llevar a cabo la utilización de las técnicas de videovigilancia por razones de seguridad en lugares públicos cuando no sea aplicable la LOPDP.

Con carácter general, a esto hay que añadir lo dispuesto en la LOPDGDD, ya que en su artículo 22, apartado primero y segundo, se relaciona con lo anterior, recogiendo:

> *«Artículo 22. Tratamientos con fines de videovigilancia.*
>
> *1. Las personas físicas o jurídicas, públicas o privadas, podrán llevar a cabo el tratamiento de imágenes a través de sistemas de cámaras o videocámaras con la finalidad de preservar la seguridad de las personas y bienes, así como de sus instalaciones.*
>
> *2. Solo podrán captarse imágenes de la vía pública en la medida en que resulte imprescindible para la finalidad mencionada en el apartado anterior...»*

De lo expuesto, se desprende que en la vía pública, cualquier entidad que no sea considerada autoridad pública y que no tenga la finalidad entre las recogidas en el artículo 1 de la LOPDP, pueden captar imágenes cuando sea imprescindible para la preservación de la seguridad de las personas y bienes o instalaciones, permitiéndose mayor extensión como se explicará para preservar la seguridad de bienes o instalaciones estratégicos o de infraestructuras vinculadas al transporte, pero que no podría implicar una captación de imágenes de un domicilio privado.

Como puede verse, la LOPDP específica las finalidades de prevención, detección e investigación de delitos sumando a la protección de los edificios e instalaciones propias; asegurar la protección de edificios e instalaciones, el uso de la videovigilancia para detectar o investigar la comisión de infracciones penales y la protección y prevención frente a las amenazas contra la seguridad pública.

Por su parte, como base legitimadora del uso de estos dispositivos para los fines recogidos en su artículo 3, la LOPSC, en su artículo 22 en cuanto al uso de la videovigilancia incluye una remisión a la legislación vigente.

> *«Artículo 22. Uso de videocámaras.*
> *La autoridad gubernativa y, en su caso, las Fuerzas y Cuerpos de Seguridad podrán proceder a la grabación de personas, lugares u objetos mediante cámaras de videovigilancia fijas o móviles legalmente autorizadas, de acuerdo con la legislación vigente en la materia.»*

En cuanto a los principios rectores en el uso de las videocámaras se establecen en los diferentes textos legales que regulan la materia. En concreto destaca el principio de proporcionalidad, como elemento básico y piedra angular del sistema, entendido en su doble vertiente de idoneidad y de intervención mínima. La proporcionalidad debe entenderse como la concurrencia del necesario equilibrio o ponderación de la medida a adoptar que afecta a los derechos fundamentales, sin violentarlos, y la finalidad que persigue, existiendo una relación medio-fin que justifique la intensidad de la medida de videovigilancia.

El principio de proporcionalidad busca otorgar una cobertura legislativa en el ámbito de actuación de las FCS. Se trata de ensalzar el ámbito protector que ejercen las FCS con respecto al libre ejercicio de los derechos y deberes fundamentales, garantizando, en definitiva, la seguridad ciudadana, en relación con lo dispuesto en el artículo 104 de la CE.

Este principio también lo encontramos en el artículo 5 del RGPD, señalando que los datos personales serán recogidos con fines determinados y serán tratados posteriormente de manera compatible con dichos fines tendentes a garantizar la seguridad de las personas, bienes e instalaciones.

El Artículo 15 de la LOPDP incorpora en su apartado segundo el principio de proporcionalidad, enunciando lo siguiente:

> «2. En la instalación de sistemas de grabación de imágenes y sonidos se tendrán en cuenta, conforme al principio de proporcionalidad, los siguientes criterios:».

Por su parte, la idoneidad, que implica la adecuación de la medida al mantenimiento de la seguridad ciudadana, por lo que debe realizarse un análisis caso por caso, en cada situación, para comprobar si concurre esta circunstancia.

El principio de intervención mínima recogido en el artículo 6.3 de la LOV exige la ponderación, en cada caso, entre la finalidad pretendida y la posible afectación a los derechos constitucionales del artículo 18 de la CE, derecho al honor, a la propia imagen y a la intimidad de las personas.

Con respecto a las videocámaras móviles se mantiene el principio de peligro concreto, al exigirse la concurrencia de ese presupuesto para su uso. No obstante, se incorpora un nuevo presupuesto que no exige per se la concurrencia de este supuesto de potencialidad dañina, sino que lo circunscribe a un evento concreto o singular que lo haga necesario. Esto es, imaginemos que se va a producir una gran concentración de personas por un acto o celebración (cumbres internacionales, manifestaciones o reuniones en lugares públicos, etc.) ¿en este caso cabe solicitar el uso de estos dispositivos móviles? A nuestro entender lo que ha pretendido el legislador al añadir este nuevo requerimiento es ampliar los supuestos autorizados de utilización.

Asimismo, se recoge el principio de minimización de datos, exigiéndose que los datos objeto de tratamiento sean adecuados, pertinentes y limitados en relación con los fines para los que son tratados. Este principio se proyecta en diversos aspectos, como serán:

- La valoración de los lugares objeto de videovigilancia.
- El número de videocámaras que se utilicen.
- Las dimensiones de las mismas.
- Los sistemas de identificación que se puedan aplicar a las imágenes o sonidos captados.

III. ACTIVIDAD DE TRATAMIENTO: LA VIDEOVIGILANCIA

A los efectos de determinar la normativa aplicable al uso de videocámaras por las FCS, es importante tener presente la finalidad del tratamiento, es decir, no es lo mismo que el tratamiento se realice para prevenir un delito, que se realice en el marco de actividades administrativas, como por ejemplo las realizadas mediante el uso de bases de datos como ADEXTTRA o, en un futuro próximo, el sistema Entry/Exit System (EES)[11]. Por tanto, los ficheros creados por las FCS que contengan datos de carácter personal recogidos para fines administrativos estarán sujetos en toda su extensión al régimen general del RGPD, la LOPDGDD y en el caso de obtención de imágenes a la LOV.

A partir del artículo 15 de la LOPDP, se regula un nuevo régimen específico de los sistemas de grabación de imágenes y sonido por las FCS con las finalidades de su artículo 1. En esta sección se fijan los principios específicos que, junto con los principios generales de tratamiento, deben servir de base a estas actuaciones cuando se lleven a cabo con las finalidades expresadas.

La citada regulación se deriva del nuevo estatuto que impone el Derecho de la Unión en esta materia, a la obligación de transponer la DDP y, a nivel interno, del mandato legal contenido en el artículo 22.6 de la LOPDGDD (sobre el que luego volveremos), al disponer lo siguiente:

> «6. *El tratamiento de los datos personales procedentes de las imágenes y sonidos obtenidos mediante la utilización de cámaras y videocámaras por las Fuerzas y Cuerpos de Seguridad y por los órganos competentes para la vigilancia y control en los centros penitenciarios y para el control, regulación, vigilancia y disciplina del tráfico, se regirá por la legislación de transposición de la Directiva (UE) 2016/680, cuando el tratamiento tenga fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública. Fuera de estos supuestos, dicho tratamiento se regirá por su legislación específica y supletoriamente por el Reglamento (UE) 2016/679 y la presente ley orgánica.*»

Esta previsión hizo necesario abordar un sistema específico de grabaciones de imágenes y sonidos por parte de los miembros de las FCS que se recoge en la LOPDP (dejando al margen, eso sí, al resto de las autoridades competentes las cuales se adaptarán a su reglamentación propia). El propósito de la regulación tan concreta ha sido garantizar la máxima protección y las más elevadas garantías en el ejercicio de los derechos de los interesados, manteniendo el equilibrio entre el uso de estos dispositivos y las finalidades de protección de la seguridad pública, los edificios e instalaciones tanto propias como públicas y de los accesos que estén bajo su custodia. Asimismo, ha perseguido salvaguardar y proteger las instalaciones útiles para la seguridad nacional; prevenir, detectar o investigar la comi-

[11] https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/smart-borders/ees_en

sión de ilícitos penales; y proteger y prevenir a los ciudadanos frente a las amenazas contra la citada seguridad pública.

Dada la evolución de la técnica y la posibilidad de llevar a cabo las grabaciones de imágenes y sonidos a través de medios como los UAS (drones) o las denominadas bodycams, que pueden afectar fácil y notablemente a los derechos de terceros, sin perjuicio de la posible vulneración de los derechos de los propios agentes actuantes en el caso de las cámaras personales, se han establecido distintos requisitos que los responsables deben tener en cuenta en cada una de las situaciones dependiendo de si los sistemas de grabación son fijos o móviles.

Se reglamentan las condiciones y plazos obligatorios para que los responsables los implanten en sus respectivas actividades de tratamiento y se dispone la inclusión imperativa de determinadas actuaciones, así como los tipos infractores de los distintos regímenes disciplinarios de las FCS en el caso de incumplimiento.

Y tal como exponíamos, se regula con cierto grado de detalle en la Sección 2.ª del capítulo II (artículos 15 a 19), el sistema de grabación de imágenes y sonidos de las FCS (artículo 15), la instalación de sistemas fijos y de dispositivos móviles (artículos16 y 17), el tratamiento y conservación de las imágenes (artículo 18), el régimen disciplinario (artículo 19) y los supuestos de aplicación especial en la Disposición Adicional Primera.

No se ha previsto la derogación expresa de la LOV, ni de su Reglamento de desarrollo, es decir del bloque normativo anterior que regulaba el régimen de videovigilancia, por lo que únicamente serán de aplicación directa o subsidiariamente en la medida que no se aplique o no contravengan lo dispuesto en la LOPDP.

En resumen, siempre que el tratamiento de datos obtenidos mediante dispositivos de videovigilancia se realice por autoridades competentes (FCS) con los fines específicos recogidos en la LOPDP, fines de prevención, detección, investigación y enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y prevención frente a las amenazas contra la seguridad pública, serán de aplicación las referidas disposiciones recogidas en la Sección 2 del Capítulo II de la Ley y en la disposición adicional primera.

En cambio, si la finalidad de la actividad de tratamiento de videovigilancia llevada a cabo por estas autoridades competentes no se encuadra en el referido ámbito, serán de aplicación las disposiciones de la LOV, Reglamento de Protección de Datos y la LOPDGDD, en concreto su artículo 22 y 89[12] en cuanto al de datos obtenidos a través de sistemas de cámaras o videocámaras.

---

[12] LOPDP: *«Artículo 89. Derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo. 1. Los empleadores podrán tratar las imágenes obtenidas a través de sistemas de cámaras o videocámaras para el ejercicio de las funciones de control de los trabajadores o los empleados públicos previstas, respectivamente, en el artículo 20.3 del Estatuto de los Trabajadores y en la legislación de función pública, siempre que estas funciones se ejerzan dentro de su marco legal y con los límites inherentes al mismo. Los empleadores habrán de informar con carácter previo, y de forma expresa, clara y concisa, a los trabajadores o los empleados públicos y, en su caso, a sus representantes, acerca de esta medida. En el supuesto de que se haya captado la comisión flagrante de un acto ilícito por los trabajadores o los empleados públicos se entenderá cumplido el deber de informar cuando existiese al menos el dispositivo al que se refiere el artículo 22.4 de esta ley orgánica. 2. En ningún caso se admitirá la instalación de sis-*

Cabe mencionar de nuevo el apartado 6 del artículo 22 de la LOPDGDD relativo al tratamiento de los datos personales procedentes de las imágenes y sonidos obtenidos mediante la utilización de cámaras y videocámaras por las FCS y por los órganos competentes para la vigilancia y control en los centros penitenciarios y para el control, regulación, vigilancia y disciplina del tráfico, el cual incide en su parte segunda en que:

> «...(...)—. *Fuera de estos supuestos, dicho tratamiento se regirá por su legislación específica y supletoriamente por el Reglamento (UE) 2016/679 y la presente ley orgáni*ca.»

En este contexto, la Disposición Adicional 8ª de la LOV recogía:

> *«La instalación y uso de videocámaras y de cualquier otro medio de captación y reproducción de imágenes para el control, regulación, vigilancia y disciplina del tráfico se efectuará por la autoridad encargada de la regulación del tráfico a los fines previstos en el texto articulado de la Ley sobre Tráfico, Circulación de Vehículos a Motor y Seguridad Vial, aprobado por Real Decreto legislativo 339/1990, de 2 de marzo, y demás normativa específica en la materia...»*

Por su parte, la Disposición Adicional Única del RLOV, establecía:

> *«1. La instalación y uso de videocámaras y de cualquier otro medio de captación y reproducción de imágenes para el control, regulación, vigilancia y disciplina del tráfico en las vías públicas, se realizará con sujeción a lo dispuesto en la disposición adicional octava de la Ley Orgánica 4/1997 y en la presente disposición.*
>
> *2. Corresponderá a las Administraciones públicas con competencia para la regulación del tráfico, autorizar la instalación y el uso de los dispositivos aludidos en el apartado anterior.*
>
> *3. La resolución que ordene la instalación y uso de los dispositivos fijos de captación y reproducción, identificará genéricamente las vías públicas o los tramos de aquéllas cuya imagen sea susceptible de ser captada, las medidas tendentes a garantizar la preservación de la disponibilidad, confidencialidad e integridad de las grabaciones o registros obtenidos, así como el órgano encargado de su custodia y de la resolución de las solicitudes de acceso y cancelación.*
>
> *La vigencia de la resolución será indefinida en tanto no varíen las circunstancias que la motivaron.*
>
> *En el ámbito de la Administración General del Estado la facultad resolutoria recaerá en el Director general de Tráfico*

---

temas de grabación de sonidos ni de videovigilancia en lugares destinados al descanso o esparcimiento de los trabajadores o los empleados públicos, tales como vestuarios, aseos, comedores y análogos. 3. La utilización de sistemas similares a los referidos en los apartados anteriores para la grabación de sonidos en el lugar de trabajo se admitirá únicamente cuando resultenrelevantes los riesgos para la seguridad de las instalaciones, bienes y personas derivados de la actividad que se desarrolle en el centro de trabajo y siempre respetando el principio de proporcionalidad, el de intervención mínima y las garantías previstas en los apartados anteriores»

4. La utilización de medios móviles de captación y reproducción de imágenes, que no requerirá la resolución a la que se refiere el apartado anterior, se adecuará a los principios de utilización y conservación enunciados en el mismo.

5. La custodia y conservación de las grabaciones y la resolución de las solicitudes de acceso y cancelación a las mismas corresponderá a los órganos que determinen las Administraciones públicas competentes. En el caso de la Administración General del Estado, corresponderá al responsable de los servicios provinciales del Organismo Autónomo Jefatura Central de Tráfico.

6. Cuando los medios de captación de imágenes y sonidos a los que se refiere esta disposición resulten complementarios de otros instrumentos destinados a medir con precisión, a los efectos de la disciplina del tráfico, magnitudes tales como la velocidad de circulación de los vehículos a motor, dichos aparatos deberán cumplir los requisitos que, en su caso, prevean las normas metrológicas correspondientes.

7. La utilización de las videocámaras contempladas en esta disposición por las Fuerzas y Cuerpos de Seguridad para fines distintos de los previstos en la misma se regirá por lo dispuesto en la Ley Orgánica 4/1997 y en el presente Reglamento.

En el caso de que dicha utilización se realice por las Unidades de Policía Judicial en sentido estricto, se estará a lo dispuesto en la Ley de Enjuiciamiento Criminal y en su normativa específica.»

Cuestiones que ahora quedan fijadas legalmente en la D.A. 1ª *«Regímenes Específicos»* de la LOPDP al enumerar y clarificar que:

«1. El tratamiento de los datos personales procedentes de las imágenes y sonidos obtenidos mediante la utilización de cámaras y videocámaras por las Fuerzas y Cuerpos de Seguridad, por los órganos competentes para la vigilancia y control en los centros penitenciarios y para el control, regulación, vigilancia y disciplina del tráfico, para los fines previstos en al artículo 1, se regirá por esta Ley Orgánica, sin perjuicio de los requisitos establecidos en regímenes legales especiales que regulan otros ámbitos concretos como el procesal penal, la regulación del tráfico o la protección de instalaciones propias.

2. Fuera de estos supuestos, dichos tratamientos se regirán por su legislación específica y supletoriamente por el Reglamento (UE) 2016/679 y por la Ley Orgánica 3/2018, de 5 de diciembre.»

Por este motivo, es importante profundizar sobre la regulación específica en la materia de videovigilancia, establecida en la LECRIM, LOPSC o LSP, ya que de las mismas se derivan distintas especificidades. Sin olvidar que, tal y como se apuntaba con anterioridad, debería adaptarse un régimen concreto, cuando en base a la legalidad aplicable, se usen sistemas de videovigilancia en el marco de situaciones donde la Guardia Civil o cualquier otra autoridad competente, realicen funciones relativas a la Defensa Nacional (ya sea en territorio nacional o en zona de operaciones).

1. Grabaciones realizadas por las Fuerzas y Cuerpos de Seguridad como Policía Judicial

Como se desprende claramente de la señalada D.A. 1ª de la LOPDP, la videovigilancia por los miembros de las Fuerzas y Cuerpos de Seguridad en cuanto

autoridades habilitadas desarrollando funciones de policía judicial se enmarca en la LECRIM. En concreto y básicamente, en los artículos 282, 588 quater a) y d) y 588 quinquies a).

El artículo 282 de la LEC detalla que:

> *«La Policía Judicial tiene por objeto y será obligación de todos los que la componen, averiguar los delitos públicos que se cometieren en su territorio o demarcación; practicar, según sus atribuciones, las diligencias necesarias para comprobarlos y descubrir a los delincuentes, y recoger todos los efectos, instrumentos o pruebas del delito de cuya desaparición hubiere peligro, poniéndolos a disposición de la autoridad judicial...»*

Artículo 588 quater a) relativo a la grabación de las comunicaciones orales directas detalla:

> *«1. Podrá autorizarse la colocación y utilización de dispositivos electrónicos que permitan la captación y grabación de las comunicaciones orales directas que se mantengan por el investigado, en la vía pública o en otro espacio abierto, en su domicilio o en cualesquiera otros lugares cerrados.*
>
> *Los dispositivos de escucha y grabación podrán ser colocados tanto en el exterior como en el interior del domicilio o lugar cerrado.*
>
> *2. En el supuesto en que fuera necesaria la entrada en el domicilio o en alguno de los espacios destinados al ejercicio de la privacidad, la resolución habilitante habrá de extender su motivación a la procedencia del acceso a dichos lugares.*
>
> *3. La escucha y grabación de las conversaciones privadas se podrá complementar con la obtención de imágenes cuando expresamente lo autorice la resolución judicial que la acuerde.»*

Artículo 588 quater d), relativo al tratamiento de las imágenes, cadena de custodia y evidencias digitales:

> *«En cumplimiento de lo dispuesto en el artículo 588 bis g, la Policía Judicial pondrá a disposición de la autoridad judicial el soporte original o copia electrónica auténtica de las grabaciones e imágenes, que deberá ir acompañado de una transcripción de las conversaciones que considere de interés.*
>
> *El informe identificará a todos los agentes que hayan participado en la ejecución y seguimiento de la medida.»*

Artículo 588 quinquies sobre captación de imágenes en lugares o espacios públicos:

> *«1. La Policía Judicial podrá obtener y grabar por cualquier medio técnico imágenes de la persona investigada cuando se encuentre en un lugar o espacio público, si ello fuera necesario para facilitar su identificación, para localizar los instrumentos o efectos del delito u obtener datos relevantes para el esclarecimiento de los hechos.*
>
> *2. La medida podrá ser llevada a cabo aun cuando afecte a personas diferentes del investigado, siempre que de otro modo se reduzca de forma rele-*

vante la utilidad de la vigilancia o existan indicios fundados de la relación de dichas personas con el investigado y los hechos objeto de la investigación.»

De conformidad con la normativa expuesta los miembros de las FCS en su función de policía judicial pueden utilizar sin autorización judicial medios de videograbación en lugares públicos para recabar los elementos probatorios necesarios.

La jurisprudencia del TS ha recogido que cuando la grabación se realiza desde la vía pública y sobre escenas que se desarrollan en el espacio público, en la medida que no se vulnera el artículo 18 de la CE, no se precisa autorización judicial si los miembros de las FCS actúan en sus funciones de policía judicial (ya sea con carácter específico o genérico)

No obstante, cuando los medios técnicos de captación de la imagen se usan junto con medios técnicos de captación de la comunicación oral se precisa una autorización judicial.

Y no hay que olvidar tampoco las referencias contenidas en los artículos siguientes:

Artículo 282 bis:

«7. En el curso de una investigación llevada a cabo mediante agente encubierto, el juez competente podrá autorizar la obtención de imágenes y la grabación de las conversaciones que puedan mantenerse en los encuentros previstos entre el agente y el investigado, aun cuando se desarrollen en el interior de un domicilio.»

En estos supuestos, la precitada Circular 4/2019, de 6 de marzo, de la Fiscal General del Estado, sobre utilización de dispositivos técnicos de captación de la imagen, de seguimiento y de localización, señala en su apartado 2, entre otras cuestiones que:

«Efectivamente, desde hace ya tiempo la jurisprudencia venía considerando legítima y no vulneradora de derechos fundamentales la filmación de escenas presuntamente delictivas que suceden en espacios o vías públicas (SSTS n.º 968/1998, de 17 julio; 67/2014, de 28 enero; 409/2014, de 21 de mayo; y 200/2017, de 27 de marzo). "Lo relevante es discernir cuando se trata de un espacio reservado a la autorización judicial, domicilio o lugar cerrado, o cuando por propia iniciativa los agentes pueden captar las imágenes cuestionadas por tratarse de 'lugares o espacios públicos', pues en estos, incluyendo con carácter general todos aquellos ajenos a la protección constitucional dispensada por el artículo 18.2 de la Constitución Española (en adelante, CE) a la inviolabilidad domiciliaria o por el artículo 18.1 a la intimidad, podrá ser decidida por propia iniciativa por los agentes de policía" (STS n.º 272/2017, de 18 de abril).

Lo que determinará, por lo tanto, la necesidad de autorización judicial será la afectación de algún derecho fundamental (inviolabilidad domiciliaria, intimidad, secreto de las comunicaciones o protección de datos), quedando limitado el ámbito de aplicación de la medida por simple iniciativa policial al resto de los supuestos. El criterio que va a determinar cuándo se afecta o no el derecho fundamental no va a ser el lugar donde se coloque el dispositivo de captación de la imagen (público o privado), sino el lugar o espacio público o privado donde se encuentre el sujeto objeto de la grabación; será este lugar, bien por estar protegido por la inviolabilidad domiciliaria, bien por generar

una razonable expectativa de privacidad (por ejemplo, el aseo de un establecimiento público), el que determine la naturaleza y alcance de la medida.»

2. Grabaciones realizadas en aplicación de Ley Orgánica de Protección de la de Seguridad Ciudadana (LOPSC)

El Artículo 21 de la LOPSC recoge las medidas de seguridad extraordinaria:

«Las autoridades competentes podrán acordar, como medidas de seguridad extraordinarias, el cierre o desalojo de locales o establecimientos, la prohibición del paso, la evacuación de inmuebles o espacios públicos debidamente acotados, o el depósito de explosivos u otras sustancias susceptibles de ser empleadas como tales, en situaciones de emergencia que las hagan imprescindibles y durante el tiempo estrictamente necesario para garantizar la seguridad ciudadana. Dichas medidas podrán adoptarse por los agentes de la autoridad si la urgencia de la situación lo hiciera imprescindible, incluso mediante órdenes verbales.»

A los efectos de este artículo, se entiende por emergencia aquella situación de riesgo sobrevenida por un evento que pone en peligro inminente a personas o bienes y exige una actuación rápida por parte de la autoridad o de sus agentes para evitarla o mitigar sus efectos.

En supuestos de urgencia, las FCS deberán actuar e intervenir en base a los Principios Básicos de Actuación del artículo 5.2.c) de la Ley Orgánica 2/1986 de Fuerzas y Cuerpos de Seguridad, con la decisión necesaria y sin demora, cuando de ella dependa evitar un daño grave, inmediato e irreparable, rigiéndose al hacerlo por los principios de congruencia, oportunidad y proporcionalidad en la utilización de los medios a su alcance.

En el artículo 22 de la misma, se hace referencia a la videovigilancia por parte de las FCS a modo de presupuesto legal en blanco o de remisión, recogiendo:

«Artículo 22. Uso de videocámaras.

La autoridad gubernativa y, en su caso, las Fuerzas y Cuerpos de Seguridad podrán proceder a la grabación de personas, lugares u objetos mediante cámaras de videovigilancia fijas o móviles legalmente autorizadas, de acuerdo con la legislación vigente en la materia.»

La LOPSC aprovechó en su artículo 36.23 a recoger como infracción grave la conducta ciudadana del uso no autorizado de imágenes o datos personales o profesionales de autoridades o miembros de las Fuerzas y Cuerpos de Seguridad que pueda poner en peligro la seguridad personal o familiar de los agentes, de las instalaciones protegidas o en riesgo el éxito de una operación, con respeto al derecho fundamental de la información. Se observa como los ciudadanos no tienen limitado la captación de imágenes, sino que tienen limitado el uso de las mismas, siempre que puedan poner en peligro la seguridad personal o familiar de los agentes, de las instalaciones. En relación con este artículo cabe mencionar la sentencia 172/2020. De 19 de noviembre de 2020, relativa al recurso de inconstitucionalidad 2896-2015, en relación con diversos preceptos de la Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana: nulidad parcial del precep-

to legal que tipifica como infracción grave el uso no autorizado de imágenes o datos personales o profesionales de autoridades o miembros de las fuerzas y cuerpos de seguridad; interpretación conforme con la Constitución de ese mismo ilícito administrativo la cual 1.º Declarar la inconstitucionalidad y la nulidad del inciso «no autorizado» del artículo 36.23 de la Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana (LOPSC).

Dado lo anterior, se elimina del artículo 36.23 de la LOPSC la mención *«no autorizado»*, al considerar que hay censura previa correspondiente al artículo 20.2 CE[13] cuando la difusión de las imágenes o datos se sometan a un previo examen de su contenido por el poder público, de forma que el uso solo se pueda realizar si este otorga una autorización previa.

3. La videovigilancia en la Ley de Seguridad Privada

El artículo 22 de la LOPDGDD es el precepto que regula los tratamientos con fines de videovigilancia. En su apartado 1 dispone que las personas físicas o jurídicas, públicas o privadas, podrán llevar a cabo el tratamiento de imágenes a través de sistemas de cámaras o videocámaras con la finalidad de preservar la seguridad de las personas y bienes, así como de sus instalaciones. Detallando a continuación determinadas condiciones, previsiones concretas sobre el ámbito de aplicación y regímenes especiales.

En su apartado 7 dispone que lo regulado en ese artículo se entiende sin perjuicio de lo previsto en la Ley 5/2014, de 4 de abril, de Seguridad Privada y sus disposiciones de desarrollo.

La LSP en el artículo 42, determina lo siguiente en relación con los servicios de videovigilancia:

> «1. *Los servicios de videovigilancia consisten en el ejercicio de la vigilancia a través de sistemas de cámaras o videocámaras, fijas o móviles, capaces de captar y grabar imágenes y sonidos, incluido cualquier medio técnico o sistema que permita los mismos tratamientos que éstas.*
>
> *2. No se podrán utilizar cámaras o videocámaras con fines de seguridad privada para tomar imágenes y sonidos de vías y espacios públicos o de acceso público salvo en los supuestos y en los términos y condiciones previstos en su normativa específica, previa autorización administrativa por el órgano competente en cada caso. Su utilización en el interior de los domicilios requerirá el consentimiento del titular.*
>
> *3. Las cámaras de videovigilancia que formen parte de medidas de seguridad obligatorias o de sistemas de recepción, verificación y, en su caso, res-*

[13] *«Artículo 20 de la Constitución Española 1. Se reconocen y protegen los derechos:*

a) A expresar y difundir libremente los pensamientos, ideas y opiniones mediante la palabra, el escrito o cualquier otro medio de reproducción.

b) A la producción y creación literaria, artística, científica y técnica.

c) A la libertad de cátedra.

d) A comunicar o recibir libremente información veraz por cualquier medio de difusión. La ley regulará el derecho a la cláusula de conciencia y al secreto profesional en el ejercicio de estas libertades.

2. El ejercicio de estos derechos no puede restringirse mediante ningún tipo de censura previa.»

puesta y transmisión de alarmas, no requerirán autorización administrativa para su instalación, empleo o utilización.

4. Las grabaciones realizadas por los sistemas de videovigilancia no podrán destinarse a un uso distinto del de su finalidad. Cuando las mismas se encuentren relacionadas con hechos delictivos o que afecten a la seguridad ciudadana, se aportarán, de propia iniciativa o a su requerimiento, a las Fuerzas y Cuerpos de Seguridad competentes, respetando los criterios de conservación y custodia de las mismas para su válida aportación como evidencia o prueba en investigaciones policiales o judiciales.

5. La monitorización, grabación, tratamiento y registro de imágenes y sonidos por parte de los sistemas de videovigilancia estará sometida a lo previsto en la normativa en materia de protección de datos de carácter personal, y especialmente a los principios de proporcionalidad, idoneidad e intervención mínima.

6. En lo no previsto en la presente ley y en sus normas de desarrollo, se aplicará lo dispuesto en la normativa sobre videovigilancia por parte de las Fuerzas y Cuerpos de Seguridad.»

Como puede observarse, la aplicación en este ámbito es únicamente subsidiaria en lo no recogido específicamente en la LSP, de manera que se regulan la videovigilancia en el ámbito de la seguridad privada, en cumplimiento del mandato contenido en la Disposición adicional novena de la Ley Orgánica 4/1997, de 4 de agosto, de utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos, que venía a disponer:

«El Gobierno elaborará, en el plazo de un año, la normativa correspondiente para adaptar los principios inspiradores de la presente Ley al ámbito de la seguridad privada.»

Como se puede observar, contenía un mandato por el que el Gobierno debía elaborar en el plazo de un año, la normativa correspondiente para adaptar los principios inspiradores de dicha norma al ámbito de la seguridad privada. Hasta la publicación de la LSP no se dio cumplimiento al mandato contenido en la LOV.

En relación con los lugares donde se puede implantar un sistema de videovigilancia se establecen en el citado artículo 42 de la LSP una serie de limitaciones:

- El consentimiento del interesado cuando la toma de imágenes y sonidos se realice en domicilios.
- Autorización administrativa cuando la toma de imágenes y sonidos se realice en vías y espacios públicos o de acceso público, salvo:
  - Lo establecido en la normativa específica en cada caso.
  - Que la medida sea obligatoria.
  - Se trate de sistemas de recepción, verificación y, en su caso, respuesta y transmisión de alarmas.

A estos supuestos debemos añadir que se trate de imágenes del espacio público que resulte imprescindible obtener para la finalidad de la vigilancia cuando no se pueda modificar la ubicación de las cámaras, según el parecer de la AEPD.

Todo sistema de videovigilancia instalado de acuerdo con la LSP tendrá que responder a una única finalidad de seguridad, teniendo como objeto la Ley la prestación de servicios para la protección de personas y de bienes. Así, el artículo 42 de la LSP establece igualmente la imposibilidad del uso de las grabaciones para un uso distinto de su finalidad.

Abundando en lo cual, la Circular 4/2019, de 6 de marzo nos indica que:

> *«Tampoco se incluyen en el ámbito de aplicación del art. 588 quinquies a las grabaciones que se realicen al amparo de las previsiones contenidas en la Ley 5/2014, de 4 de abril, de Seguridad Privada. Aquí, las diferencias son mayores, ya que la grabación no se realiza por las Fuerzas y Cuerpos de Seguridad del Estado y no se captan imágenes que tengan lugar en espacios públicos; estas grabaciones estarán a cargo de vigilantes de seguridad o, en su caso, guardas rurales, y no podrán tomar imágenes y sonidos de vías y espacios públicos o de acceso público. "Las grabaciones realizadas por los sistemas de videovigilancia -conforme al art. 42 de la Ley- no podrán destinarse a un uso distinto del de su finalidad. Cuando las mismas se encuentren relacionadas con hechos delictivos o que afecten a la seguridad ciudadana, se aportarán, de propia iniciativa o a su requerimiento, a las Fuerzas y Cuerpos de Seguridad competentes, respetando los criterios de conservación y custodia de las mismas para su válida aportación como evidencia o prueba en investigaciones policiales o judiciales".*
>
> *Las grabaciones obtenidas por medio de sistemas de videovigilancia pueden afectar al contenido del derecho fundamental a la protección de datos de carácter personal. Para que resulten ajustadas a la Ley y, en consecuencia, aptas para su valoración como prueba por un tribunal, será necesario que las mismas se ajusten a las previsiones contenidas en el art. 22 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y legislación complementaria, sin que sea precisa una información descriptiva y detallada de los fines para los que se han instalado las cámaras (en este sentido, la STC n.º 39/2016, de 3 de marzo).»*

Como puede apreciarse, en este título resulta relevante la regulación de los servicios de videovigilancia y de investigación privada, ya que se trata de servicios que potencialmente pueden incidir de forma directa en la esfera de la intimidad de los ciudadanos. En el segundo caso, desde el ánimo de compaginar los diversos intereses en juego, se abordan cuestiones tan delicadas como la legitimidad del encargo, el contenido del informe de investigación o el deber de reserva profesional.

IV. INSTALACIÓN DE SISTEMAS FIJOS DE VIDEOVIGILANCIA

La instalación de dispositivos fijos se regula en el artículo 16 de la LOPDP.

Dada la proliferación y sistemas de grabación de imágenes, la primera cuestión a la que se debería atender es cuál es la definición de videocámara fija. En este marco se debe entender por videocámara fija aquella anclada a un soporte fijo o fachada, aunque el sistema de grabación se pueda mover en cualquier dirección, cuestión esta que suscitó algún debate entre las autoridades competentes para autorizar dichas instalaciones a la luz de la LOV. Como se observa, el legislador ha querido clarificar esta cuestión, no sabemos si con acierto o no, si bien, da carta de naturaleza a que los sistemas fijos puedan articularse y, en caso necesario, tomar imágenes con un margen más amplio de «movilidad» sin tener que acudir únicamente al zoom.

En las vías o lugares públicos donde se instalen videocámaras fijas, el responsable de tratamiento deberá realizar una valoración de los principios de tratamiento y se analizará en todos los extremos la actuación pretendida desde el diseño de la misma, evaluando específicamente el citado principio de proporcionalidad en su doble versión de idoneidad e intervención mínima. Asimismo, en función de la finalidad perseguida y del nivel de perjuicio que se pueda derivar para la ciudadanía, deberá llevar a cabo un análisis de los riesgos o en caso de estimarse una evaluación de impacto de protección de datos relativa al tratamiento.

Con esta nueva redacción se desprende que lo que se persigue sería facilitar la instalación de dispositivos fijos, terminando con el supuesto habilitante recogido en la LOV, existencia de un *«riesgo razonable»* y el régimen de autorización previa. Toda la carga y obligación de cumplir la normativa y de demostrar que esta se cumple, se traslada al responsable de tratamiento quien, considerando todos los extremos expuestos, deberá valorar la idoneidad de instalación de un dispositivo o sistema de grabación fijo. O lo que es lo mismo, debe cumplir totalmente con el concepto de diligencia debida o proactividad reflejado anteriormente.

El referido análisis de riesgos o la evaluación de impacto de protección de datos, consistentes en un estudio general del tratamiento, una evaluación del peligro para los interesados y una ponderación entre la finalidad perseguida y la vulneración de derechos derivada de la instalación del sistema fijo de videovigilancia resultará de carácter ineludible. De la redacción propuesta puede desprenderse que se debe comprobar si la instalación de un sistema fijo de videovigilancia, como medida que restringe derechos fundamentales, se ajusta a los principios, cumple con la normativa y no genera un nivel de riesgo inasumible para las personas. De todos modos, en el caso de duda por parte del responsable, la propia LOPDP facilita la actuación a llevar cabo. Puesto que tanto si la EIPD llevada a cabo indica que el tratamiento entraña un alto nivel de riesgo, a falta de medidas adoptadas por el responsable para mitigar el riesgo o los posibles daños como si el tipo de tratamiento pueda generar un alto nivel de riesgo para los derechos y libertades de los interesados, en particular, cuando se usen tecnologías, mecanismos o procedimientos nuevos, el responsable debe consultar previamente a la Autoridad de Protección de datos competente antes de proceder al tratamiento.

Este artículo se aplicará asimismo cuando las Fuerzas y Cuerpos de Seguridad utilicen instalaciones fijas de videocámaras de las que no sean titulares y exista, por su parte, un control y dirección efectiva del proceso completo de tratamiento.

Se excluye el control preventivo de las entidades locales previsto en su legislación reguladora básica, y el ejercicio de las competencias de las diferentes Administraciones públicas, sin perjuicio de que deban respetar los principios de la legislación vigente en cada ámbito material de la actuación administrativa. Esta cuestión ya figuraba en la LOV y viene a ser una previsión para que no se pueda someter a autorización previa por parte de autoridades distintas a las competentes la instalación de estos sistemas por normativas municipales que no tengan relación con la seguridad pública; no obstante, como señala el legislador, esto no es óbice para que se cumplan escrupulosamente las normas que se deban aplicar (véase patrimonio histórico, seguridad y calidad en la edificación, licencia de obras, etc...).

Los propietarios y, en su caso, los titulares de los derechos reales sobre los bienes afectados por estas instalaciones, o quienes los posean por cualquier título, están obligados a facilitar y permitir su instalación y mantenimiento, sin perjuicio de las indemnizaciones que procedan.

Se incluye un derecho de información a los ciudadanos quienes deberán ser informados de manera clara y permanente de la existencia de estas videocámaras fijas, sin especificar su emplazamiento, así como de la autoridad responsable del tratamiento ante la que poder ejercer sus derechos (sin perjuicio de facilitar toda la información posible en esa primera capa y de informar donde pueden obtener más información). Como ejemplo, se adjuntan en las páginas posteriores los carteles informativos de las instalaciones de este Departamento en sus sedes de Madrid.

En definitiva, la Ley 7/2021 supone un cambio de sistema en cuanto a la instalación de sistemas de videovigilancia fijos, introduciendo numerosos cambios con respecto a la LOV, los cuales pueden resumirse en los siguientes puntos:

- En nuestra opinión, se suprime el régimen de autorización establecido en la LOV, eliminando las competencias de las Delegaciones del Gobierno y la intervención de la Comisión de Garantías de la Videovigilancia, por lo que cabe concluir la derogación tácita de todas las competencias de estas Comisiones en lo que respecta a la instalación de sistemas fijos de videovigilancia a estos fines. Esta valoración de los autores, no es compartida por varios organismos y entidades. La Fiscalía.
- Se elimina el supuesto habilitante de «existencia de un riesgo razonable» para la instalación de sistemas fijos de videovigilancia.
- La decisión de instalación de un determinado sistema fijo de videovigilancia depende del responsable de tratamiento, quien llevará a cabo un análisis de los riesgos o una evaluación de impacto para decidir sobre la idoneidad de la instalación de un determinado dispositivo fijo.

V. DISPOSITIVOS MÓVILES

El uso de estos dispositivos móviles se regula en el artículo 17 de la LOPDP, estableciendo un sistema que permite el uso de estos dispositivos de toma de imagen y sonido, en casos donde concurra un peligro o un evento concreto.

Como se observa, los presupuestos fácticos son dos:

De un lado la concurrencia de peligro, es decir, la aparición o existencia de un agente dañino (situación, circunstancia o persona) que pueda minusvalorar o afectar a los bienes objeto de protección. No existe una única definición de peligro, si acudimos al Diccionario de la Academia Española el concepto sería: *«Riesgo o contingencia inminente de que suceda algún mal.»* Esta definición eminentemente léxica o conceptual ya facilita algunas directrices de cómo interpretar y aplicar esta parte del precepto analizado.

En la Ley 17/2015, de 9 de julio, del Sistema Nacional de Protección Civil, en su artículo 2.1 se define el peligro en su ámbito como el:

> *«Potencial de ocasionar daño en determinadas situaciones a colectivos de personas o bienes que deben ser preservados por la protección civil.»*

Y como último ejemplo, en la Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana, amén de fijar en su parte expositiva que: *«La Constitución Española de 1978 asumió el concepto de seguridad ciudadana (artículo 104.1), así como el de seguridad pública (artículo 149.1.29.ª). Posteriormente, la doctrina y la jurisprudencia han venido interpretando, con matices, estos dos conceptos como sinónimos, entendiendo por tales la actividad dirigida a la protección de personas y bienes y al mantenimiento de la tranquilidad ciudadana. Es a la luz de estas consideraciones como se deben interpretar la idea de seguridad ciudadana y los conceptos afines a la misma, huyendo de definiciones genéricas que justifiquen una intervención expansiva sobre los ciudadanos en virtud de peligros indefinidos, y evitando una discrecionalidad administrativa y una potestad sancionadora genéricas.»; e*n su parte dispositiva, utiliza y fija este criterio de peligro en al menos quince ocasiones. Las más relevantes quizás sean las referencias que se recogen en sus artículos 4.3, 18 y 21.

Pero todas estas alusiones hacen referencia a una situación que no exige resultado dañino sino una potencialidad de menoscabo o perjuicio para los bienes jurídicos protegidos que no tiene por qué ser de carácter grave o muy grave, sino derivar una probabilidad de causar mal a las personas y entidades a las que se pretende dotar de seguridad.

Por otro lado, la concurrencia de un evento concreto que quede bajo la competencia de las FCS, estos eventos pueden ser fijos, periódicos, de duración determinada o indeterminada. Ejemplos serían una competición deportiva, una concentración de personas, las visitas de personalidades, una cumbre internacional, un festival de música de varios días, etc.

En ambos casos, lo relevante a nivel policial, sería analizar el tratamiento necesario y motivar la petición de autorización a la autoridad solicitante con todos los argumentos que concurran tanto en el supuesto del «agente dañino» como el «evento concreto».

Además de este presupuesto material, el legislador ha realizado una previsión que va más allá incluso de las prevenciones legales que se impone en materia de investigación criminal. Esto es, el uso de estos dispositivos habilita la toma de imagen y sonido de manera conjunta con el objetivo de acreditar los hechos captados en toda su extensión, pero en este caso, no exige el requisito de autorización judicial como en el caso amparado por el artículo 588 quater a) de la LECRIM.

En base a la interpretación que debe darse esta norma en correspondencia con el artículo 3 del Código Civil, a resultas de lo que se resuelva a futuro por las Autoridades Judiciales, es obvio que si por ejemplo un dron es considerado un dispositivo de grabación móvil y este vuela a una altitud que no permite emplear el uso de sistema de grabación conjunta de imagen y sonido, este podrá utilizarse si cumple con las dimensiones y condiciones de seguridad aunque no sea posible obtener las conversaciones orales o sonidos ambientes.

Como se observa pues, se establece un sistema de autorización previa por la persona titular de la Delegación o Subdelegación del Gobierno, quien de forma motivada deberá atender a la naturaleza de los eventuales hechos susceptibles de filmación, de conformidad con los principios de tratamiento y proporcionalidad.

En orden a valorar la concesión de la autorización, serán de aplicación los elementos contenidos en la solicitud, junto con los principios de proporcionalidad y los principios de tratamiento en la línea de lo previsto en el artículo 6 de la Ley 7/2021:

> *«1. Los datos personales serán:*
> *a) Tratados de manera lícita y leal.*
> *b) Recogidos con fines determinados, explícitos y legítimos, y no serán tratados de forma incompatible con esos fines.*
> *c) Adecuados, pertinentes y no excesivos en relación con los fines para los que son tratados.*
> *d) Exactos y, si fuera necesario, actualizados. Se adoptarán todas las medidas razonables para que se supriman o rectifiquen, sin dilación indebida, los datos personales que sean inexactos con respecto a los fines para los que son tratados.*
> *e) Conservados de forma que permitan identificar al interesado durante un período no superior al necesario para los fines para los que son tratados.*
> *f) Tratados de manera que se garantice una seguridad adecuada, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental. Para ello, se utilizarán las medidas técnicas u organizativas adecuadas...»*

Se observa como para este supuesto se ha modificado la base habilitante recogida en la LOV, *«existencia de un peligro concreto»*, ya que se elimina la concreción, y se añade la concurrencia de una circunstancia nueva, la existencia de un *«evento concreto»*[14] que haga necesario su uso.

[14] Sentencia de TS 27 /02/1996 se entiende por *«peligro concreto»* la instalación de un sistema fijo ante la celebración de una manifestación en la que se tiene constancia de la concurrencia de grupos violentos.

Además, se mantiene la necesidad de obtener autorización previa en la misma línea de lo recogido en el Reglamento LOV (artículo 6), resultando de aplicación todas las disposiciones que no contradigan la LOPDP. En este sentido, de no implementarse modificaciones legislativas adicionales, se mantendrían las competencias de las Comisiones de Garantías de la Videovigilancia[15] con respecto a las videocámaras móviles, por lo que si la resolución autoriza el uso de videocámaras móviles, se pondría en conocimiento de la referida Comisión en el plazo máximo de 72 horas a contar desde su adopción, por cualquier medio telemático, informático o documental que acredite su recepción. Pero todas estas cuestiones se irán adecuando en función de la aplicación de la LOPDP y de la normativa que la desarrolle.

La resolución del Delegado del Gobierno pondrá fin a la vía administrativa y contra la misma cabrá interponer potestativamente recurso de reposición o impugnarla directamente ante el orden jurisdiccional contencioso-administrativo. Contra la resolución del Subdelegado del Gobierno podrá interponerse recurso de alzada ante el Delegado del Gobierno.

El plazo de vigencia de la autorización se limita a 1 mes, prorrogable por otro mes adicional. Se observa cómo se ha reducido notablemente el plazo de autorización, pasando de un plazo máximo de 1 año a 1 mes. En la medida que no se publiquen novedades al respecto, se entiende de aplicación las disposiciones del Reglamento LOV relativas a la renovación de las autorizaciones, por lo que, a nuestro juicio y para garantizar el procedimiento, debería solicitarse la renovación de la autorización con una antelación mínima correspondiente a la mitad del tiempo autorizado. Si no se formula la solicitud de renovación en los plazos señalados en el apartado anterior, habrá de tramitarse como una nueva autorización.

---

[15] Cabe tener presente que hasta la fecha son de aplicación las disposiciones de la LOV y su Reglamento que no contravengan la Ley 7/2021, por lo que las Comisiones de Garantías de la Videovigilancia siguen ejerciendo aquellas funciones en materia de autorización de uso de videocámaras móviles por las Fuerzas y Cuerpos de Seguridad. En concreto, de conformidad con el artículo 16 b), c), d), e), f), g) y h).

Artículo 16. Competencias de las Comisiones de Garantías de la Videovigilancia. Corresponde a las Comisiones de Garantías de la Videovigilancia ejercer las siguientes competencias:

b) Ser informada de las resoluciones de autorización de videocámaras móviles y del uso excepcional de las mismas, previstos en el apartado 2 del artículo 5 de la Ley Orgánica 4/1997.

c) Ser informada, al menos con periodicidad quincenal, de la utilización que se haga de videocámaras móviles.

d) Recabar en cualquier momento, de las Fuerzas y Cuerpos de Seguridad, el soporte físico de las grabaciones efectuadas por videocámaras móviles y emitir un informe al respecto.

e) Informar, a petición de las autoridades competentes, sobre la adecuación de cualquier registro de imagen y sonido obtenidos mediante videocámaras móviles a los principios enunciados en el artículo 6 de la Ley Orgánica 4/1997.

f) Ordenar la destrucción de las grabaciones cuando, en el ejercicio de sus competencias, constaten el incumplimiento de los criterios y principios establecidos en la Ley Orgánica 4/1997.

g) Requerir de las autoridades responsables la información necesaria para el ejercicio de sus funciones.

h) Formular cuantas recomendaciones estime oportunas en el ámbito de sus competencias.

Se contempla otro supuesto habilitante que permite en los casos de urgencia o necesidad inaplazable que el responsable operativo de las FCS competentes pueda determinar su uso sin autorización previa, siendo comunicada tal actuación con la mayor brevedad posible, y siempre en el plazo de 24 horas, al Delegado o Subdelegado del Gobierno o autoridad competente de las Comunidades Autónomas. Este régimen excepcional pivota la responsabilidad de la toma de decisión al responsable operativo de las FCS, lo cual deberá ser determinado por los procedimientos internos oportunos de los distintos organismos.

De la normativa expuesta, cabe señalar las siguientes novedades introducidas por la LOPDP en cuanto a dispositivos móviles:

- Se mantiene un sistema de autorización previa por la persona titular de la Delegación o Subdelegación del Gobierno, salvo en los casos de urgencia o necesidad inaplazable.
- Deben concurrir dos supuestos habilitantes, recogiéndose dos supuestos, existencia de un peligro, al que se añade la concurrencia de un *«evento concreto»*.
- Se reduce de manera exponencial el plazo de autorización, plazo máximo de 1 mes con una prórroga de 1 mes.
- Se limita el uso del supuesto habilitante sin autorización previa en casos de urgencia máxima, recogiendo que en los casos de urgencia o necesidad inaplazable será el responsable operativo de las Fuerzas y Cuerpos de Seguridad competentes quien pueda determinar su uso sin autorización previa
- La LOV recogía un supuesto habilitante para casos excepcionales de urgencia máxima o de imposibilidad de obtener a tiempo la autorización indicada en razón del momento de producción de los hechos o de las circunstancias concurrentes, pudiendo obtener imágenes y sonidos con videocámaras móviles, pero dando cuenta de ello a la autoridad autorizante.
- En todos los casos, el responsable del tratamiento deberá acreditar la diligencia debida en los tratamientos con un sistema de control sólido y eficaz a través de las correspondientes políticas de privacidad y protocolos de actuación.
- En definitiva, se observa como la norma, a través de las novedades introducidas, pretende ajustar a determinadas circunstancias los supuestos de uso de estos dispositivos móviles.

La autorización en el caso de cuerpos de policía propios de las Comunidades Autónomas que tengan y ejerzan competencias asumidas para la protección de las personas corresponderá a sus órganos correspondientes, así como para las dependientes de las Corporaciones locales radicadas en su territorio. En el caso catalán, es el Director de Seguridad Ciudadana el que autoriza dichas resoluciones y autorizaciones (artículo 12 del Decreto catalán 134/1999[16]) y los Directores del Departamento de Interior en el caso del País Vasco (artículo 2 del Decreto 168/1998[17]).

[16] Decreto 134/1999, de 18 de mayo, de regulación de la videovigilancia por parte de la policía de la Generalidad y de las policías locales de Cataluña.

[17] DECRETO 168/1998, de 21 de julio, por el que se desarrolla el régimen de autorización y utilización de videocámaras por la Policía del País Vasco en lugares públicos regulado en la Ley Orgánica 4/1997, de 4 de agosto.

1. Uso de cámaras móviles personales por las Fuerzas y Cuerpos de Seguridad

En multitud de intervenciones policiales se puede observar como los policías actuantes portan cámaras móviles personales o *bodycam*, surgiendo la pregunta de en qué supuestos es legal su uso. Existen multitud de seguidores y detractores del uso de estos dispositivos portátiles, por lo que resulta de especial interés analizar su encaje en la normativa española.

En primer lugar, las *bodycam* entrarían en el ámbito de aplicación de la normativa sobre dispositivos móviles, por lo que su uso, en principio sería legal y correcto siempre que se respete el sistema autorización previa establecido para estos dispositivos o en los supuestos de urgencia o necesidad inaplazable.

La Agencia Española de Protección de Datos en consulta planteada sobre si resulta conforme a la normativa de protección de datos que la policía local, en el ejercicio de sus funciones de policía judicial en sentido genérico y en casos excepcionales de máxima urgencia, capten imágenes por cualquier medio a su alcance (videocámaras domésticas y teléfonos móviles) dando cuenta en el plazo de 72 horas mediante informe motivado al máximo responsable provincial de las FCS y la Comisión constituida por la LOV al efecto con la entrega de dichas imágenes cuando la Comisión lo solicite, ha informado que:

> *«En lo que respecta a la aplicación de la normativa de protección de datos al supuesto planteado, debe tenerse en cuenta que el RGPD determina en su artículo 32, denominado "seguridad del tratamiento" lo siguiente: 1. Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:*
>
> *a) la seudonimización y el cifrado de datos personales;*
>
> *b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;*
>
> *c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;*
>
> *d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.*
>
> *2. Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.»*

En definitiva, señalan que debe examinarse en profundidad si tales cámaras domésticas y teléfonos móviles pueden garantizar la seguridad de los datos de forma que no se produzcan pérdidas o alteraciones de los datos y, muy especialmente, dada la generalización de uso de dispositivos inteligentes, la posibilidad de acceso por terceros a los datos en ellas almacenados.

Por tanto, en líneas general teniendo en cuenta los riesgos señalados debe considerarse que el uso de cámaras o móviles personales de los agentes no garantiza la seguridad de los datos, en tanto que los usos privados que cada agente pueda realizar con sus propios dispositivos no resultan compatibles con las medidas de seguridad que para el ejercicio de las funciones de policía judicial deben adoptarse por los responsables del fichero policial del que formarán parte tales grabaciones. Por este motivo, es totalmente desaconsejable el uso de estos dispositivos no oficiales, no sólo porque se puedan incumplir las medidas de seguridad oportunas y se incremente notablemente el riesgo de sufrir una brecha de seguridad, sino que además el tratamiento posterior de lo grabado tendría poco ajuste a la normativa o procedimientos que regulan la aportación como evidencias digitales a los procesos judiciales o administrativos oportunos.

Pero esta cuestión no acaba con la mera toma de las imágenes con dispositivos particulares, si no que la AEPD[18] ha concluido que, en estos supuestos, el tratamiento posterior de los datos (imágenes) y su publicidad en medios de comunicación o redes sociales constituye una infracción grave a la normativa de protección de datos en base a las siguientes consideraciones:

Como primera cuestión entiende que un miembro de las Fuerzas y Cuerpos de Seguridad que graba imágenes durante su servicio no puede ser considerado un tercero en base a la definición que de éste recoge el RGPD: *«tercero»: persona física o jurídica, autoridad pública, servicio u organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable o del encargado;»* Y, por lo tanto, entiende que los tratamientos de datos no se realizan únicamente por el responsable o el encargado del tratamiento, sino que el número de usuarios que tratan datos personales en cualquier Administración pública es equivalente al número de empleados públicos de la misma.

Igualmente recuerda la Agencia que el modelo de protección de los datos anterior basado en la LOPD se basaba en:

> *«un esquema "estático" de las medidas de seguridad a implantar, en función de la tipología de los datos tratados, se buscaba evitar la infracción de los derechos de los interesados como obligación principal, pero con el paradigma actual, basado en el concepto de diligencia debida, se busca la anticipación a la infracción o lesión de derechos, el cumplimiento con antelación para evitar así la lesión o infracción del derecho o libertad del interesado. Si bien, la normativa aplicable no enumera específicamente cuáles sean esas medidas de seguridad a implantar, no se centra en la información perteneciente a la organización, sino que se vincula especialmente a la protección de los datos de las personas físicas, exigiendo una responsabilidad proactiva, y no una responsabilidad reactiva, como sucedía en el modelo anterior. Este enfoque proactivo en la «implementación permanente» de las medidas de seguridad, implica que las mismas ya no son estáticas (como en el modelo anterior), sino dinámicas, correspondiendo al responsable de tratamiento determinar en cada momento cuáles de aquellas medidas de seguridad son necesarias para*

[18] Expediente Nº: PS/00392/2020

garantizar la confidencialidad, la integridad y la disponibilidad de los datos personales, siendo el primer paso llevar a cabo un análisis de riesgos.

Una vez evaluadas tales amenazas, el responsable podrá determinar cuáles son las medidas más apropiadas para mitigar o eliminar los riesgos para el tratamiento de datos que puedan surgir y afectar a los derechos y libertades de las personas físicas.

En consecuencia, se exige una responsabilidad proactiva, en lugar de la responsabilidad reactiva (enfoque basado en riesgos), debiéndose actuar con carácter preventivo, tener la diligencia debida para evitar tratamientos o incumplimientos no deseados en la protección de los intereses de los ciudadanos en el ámbito de su privacidad.

En este contexto, los miembros de las FCS dependientes del responsable del tratamiento puede realizar un tratamiento de los datos que no sea conforme con la normativa de protección de datos personales, sea a través de los medios proporcionados o de otros, por lo que la formación en materia de privacidad debe ser integral para la práctica totalidad de miembros de la organización.

El responsable debe establecer información y formación de sus empleados en la materias, directrices y difusión de la información sobre tratamientos de datos, de modo que se consiga una aplicación uniforme en su ámbito.

Así y todo, los empleados, y cargos directivos deben considerar antes de proceder a un tratamiento de datos, especialmente si es distinto del habitual, o novedoso, por interpretación o por situación concreta, llevar a cabo antes una consulta al responsable del tratamiento. Este deberá emitir normas a sus empleados y centros directivos para coordinar aspectos básicos de los tratamientos de datos."

Aparte del conocimiento que se ha de proporcionar y se presupone a los policías sobre la captación de imágenes en vías públicas por las Fuerzas y Cuerpos de Seguridad, que se rige por su legislación específica (LOPDP o LOV según la finalidad del tratamiento) dispone la AEPD que:

«...lógicamente se debería haber informado y previsto las consecuencias del uso de dispositivos móviles personales. Sobre estos, salvo el uso que se pueda hacer de los denominados institucionales para el ejercicio de las funciones en los supuestos en que puedan ser precisos, se debe indicar que, su uso, como cámaras o móviles personales de los agentes para captación de imágenes en el desarrollo de la labor profesional, no garantiza la seguridad de los datos, en tanto que los usos privados que cada agente pueda realizar con sus propios dispositivos no resultan compatibles con las medidas de seguridad que para el ejercicio de las funciones de policía deben adoptarse por los responsables del tratamiento, debiendo acomodar y prever concretas responsabilidades y sanciones en su caso. En este caso, se acredita que no existen tales medidas que han supuesto una intromisión no legítima en el derecho de protección de datos del reclamante.

En este caso, no se acredita que el reclamado dispusiera de medidas implantadas sobre uso de dispositivos personales en relación con la realización de sus tareas, donde advirtiera de su régimen de uso y sanción, o la no necesidad ni proporcionalidad de grabación de imágenes como la que ha sido objeto de esta reclamación. El régimen de diligencia en el cumplimiento de los principios del tratamiento de datos se relaciona con la adopción de estos protocolos, considerando que se pueden afectar derechos de los ciudadanos. Se acredita la infracción de este artículo.

> *Por lo demás, el inicio del proceso disciplinario, que es solo una parte de la política de cumplimiento normativo en la organización, se revela tardía, y reactiva, pues ha sido con ocasión de la práctica de pruebas, cuando se acredita que no existe especificidad relativa a las medidas de seguridad en el desarrollo de las tareas encomendadas en función con los riesgos y dispositivos.»*

Como conclusión se debe inferir que el uso de dispositivos privados de videograbación por parte de los miembros de las FCS en el desarrollo de su labor y cualquiera otro tratamiento posterior de las imágenes, constituye una infracción a la normativa de protección de datos personales.

En otro orden de cosas, en el caso de que se utilizasen dispositivos inteligentes que se hayan entregado de dotación con carácter oficial para su uso con fines policiales, deberán adoptarse todas las precauciones para cumplir con todos los presupuestos apuntados en este apartado y con todas las dimensiones de seguridad, principalmente la de garantizar la integridad de los datos e impedir accesos indebidos o *«brechas»* en los sistemas que afecten a los datos que con ellos se capten, pero sin perder de vista la *«disponibilidad»* y la *«integridad»* de las imágenes y, en su caso, sonidos. De manera que, los datos o evidencias derivadas de su uso puedan ser aportados a los distintos procedimientos con todas las garantías. De lo anterior, se desprende que el uso generalizado de estos dispositivos puede implicar en el futuro, riesgos derivados de la privacidad de los sujetos grabados o el tratamiento de la ingente cantidad de datos, por lo que pudiese ser de interés una regulación más específica.

Con base en la normativa actual, cabría el uso puntual y en momentos concretos de dispositivos oficiales que asegurasen el cumplimiento de las citadas medidas de seguridad, pero en cualquier caso sería de aplicación el procedimiento de autorización previsto en el artículo 17 de la LOPDP, pudiendo la Delegación del Gobierno autorizar, si la petición cumple los requisitos exigidos por la ley, a los miembros de las FCS a usar un tipo concreto de dispositivo, para un fin específico y durante un periodo temporal acotado en la autorización, pero en ningún caso la normativa actual permite el uso sine die o el uso a discreción del criterio de los propios agentes.

Aunque aún no existe una legislación específica sobre el uso de medios de grabación individuales, recordemos que también resulta de aplicación la normativa de protección datos, la LECRIM y la LOPSC.

De hecho, la AEPD ha venido a señalar en estos casos de utilización de dispositivos oficiales en determinadas circunstancias alguna matización que es relevante incluir en esta obra. En el procedimiento nº: PS/00470/2021[19] viene a concluir lo siguiente:

> *«Por tanto, con arreglo a las evidencias que se disponen en este momento, se considera que la utilización del teléfono móvil oficial de la unidad actuante para la toma de fotografías del DNI de los reclamantes, en las circunstancias tan excepcionales como las expuestas anteriormente, cumple con el principio de minimización del dato, recogido en el artículo 5.1.c) del RGPD, más aún*

[19] https://www.aepd.es/es/documento/ps-00470-2021.pdf

cuando las mismas fueron eliminadas del dispositivo una vez cumplido el objetivo para el que fueron borradas, no quedando ningún rastro de las mismas en ningún fichero de la D.G. de la Policía.»

Como se ha analizado, la normativa en materia de protección de datos delimita sustancialmente el uso de las cámaras unipersonales policiales, dificultando el uso de estos dispositivos, ya que considera que su uso generalizado puede afectar los derechos de los ciudadanos, derechos que sólo pueden verse perturbados en determinados supuestos y con determinadas garantías.

2. Los drones como dispositivos móviles de videovigilancia

Los UAS (*Unmanned Aircraft Systems o Sistemas de Aeronaves No Tripuladas*) comúnmente denominados drones o según la normativa vigente en nuestro país[20] RPA (*aeronave pilotada por control remoto por sus siglas en inglés Remotely Piloted Aircraft*), son sistemas que pueden tratar datos de carácter personal, principalmente cuando llevan instalados sensores para grabar audio o video, lo que les convierte en una herramienta básica para la seguridad pública y por ello, suponen un reto desde el punto de vista de la protección de datos y la intimidad.

Algunos ejemplos de equipos que podrían afectar a la intimidad y la protección de los datos equipados en estos dispositivos, que se contiene el *«Dictamen 01/2015, sobre cuestiones relativas a la intimidad y las protección de datos en la utilización de drones»*[21] serían:

- Equipos de grabación de imágenes: cámaras inteligentes de distancia focal fija o variable, capaces de almacenar y transmitir imágenes en directo, con funciones de reconocimiento facial a bordo o en tierra, lo que permite a los drones identificar y seguir a determinadas personas, objetos o situaciones, identificar pautas de movimiento o leer matrículas de vehículos con una visión de 360º, detectar la energía térmica emitida por un blanco, volar y grabar imágenes en condiciones de poca visibilidad (por niebla, humo o escombros) o durante la noche.
- Equipos de detección: sensores optoelectrónicos, lectores de infrarrojos y radares de apertura sintética para identificar objetos, vehículos y embar-

[20] El Real Decreto 1036/2017, de 15 de diciembre, por el que se regula la utilización civil de las aeronaves pilotadas por control remoto, y se modifican el Real Decreto 552/2014, de 27 de junio, por el que se desarrolla el Reglamento del aire y disposiciones operativas comunes para los servicios y procedimientos de navegación aérea y el Real Decreto 57/2002, de 18 de enero, por el que se aprueba el Reglamento de Circulación Aérea, está en su fase final pero aún no se ha publicado el instrumento que lo sucederá de conformidad con la normativa de la Unión Europea (El proyecto de Real Decreto por el que se completa el régimen jurídico para la utilización civil de sistemas de aeronaves no tripuladas, y se modifican diversas disposiciones aeronáuticas civiles se puede consultar en la página web del Ministerio de Transportes, Movilidad y Agenda Urbana: https://www.mitma.gob.es/el-ministerio/buscador-participacion-publica/proyecto-de-real-decreto-por-el-que-se-completa-el-regimen-juridico-para-la-utilizacion-civil-de-sistemas-de-aeronaves-no-tripuladas-y-se-modifican)

[21] *«Dictamen 01/2015 sobre las cuestiones relativas a la intimidad y la protección de los datos en la utilización de drones»* del Grupo de Trabajo del Artículo 29. Versión 16 de junio de 2015.

caciones y obtener información sobre su posición y su rumbo, incluso detrás de paredes, humo u otros obstáculos.[22]

- Equipos de radiofrecuencia: antenas que captan la localización de los puntos de acceso WiFi o estaciones celulares, fotoceldas y receptores de IMSI utilizados por los servicios con funciones coercitivas para controlar teléfonos y redes móviles o por proveedores de servicios para transmitir comunicaciones entre usuarios de terminales y redes.
- Sensores específicos para la detección de trazas nucleares, trazas biológicas, material químico o artefactos explosivos.

En este Dictamen se reitera que pese a que las repercusiones que el uso de estas aeronaves puede tener en la intimidad y la libertad de las personas difieren de los impactos de los sistemas de CCTV, puede haber circunstancias en las que las disposiciones jurídicas nacionales aplicables a los sistemas de CCTV también se apliquen al uso de drones, en particular cuando estos se utilizan con fines de vigilancia por videocámara.

En concreto, en cuanto a la protección de datos personales en el ámbito policial y de seguridad, se opina que:

> *«Los drones pueden representar una transformación fundamental de las prácticas de los servicios con funciones coercitivas, en particular en lo referente al papel que desempeñan los datos para orientar las acciones en este sentido, desde el seguimiento de una persona hasta el establecimiento de objetivos para la revisión de las vidas y las actividades de una población determinada mediante una vigilancia continua. Así pues, el uso de drones manejados directamente por la policía u otras autoridades con funciones coercitivas (o su solicitud de acceso a datos recogidos por drones manejados por entidades privadas para sus propios fines) crea riesgos elevados para los derechos y las libertades de los individuos e interfiere directamente en los derechos al respeto de la vida privada y la protección de los datos personales previstos en el artículo 8 del Convenio Europeo de Derechos Humanos ("el CEDH") y los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea ("la Carta").*
>
> *Por lo tanto, con arreglo al artículo 52, apartado 1, de la Carta y al artículo 8, apartado 2, del CEDH, esta limitación del ejercicio de los derechos y libertades reconocidos por la Carta deberá ser establecida por la ley ("prevista por la ley"), cuando sea necesaria y responda efectivamente a objetivos de interés general reconocidos por la Unión o a la necesidad de protección de los derechos y libertades de los demás ("perseguir los objetivos legítimos establecidos en el artículo 8, apartado 2 y ser necesaria en una sociedad democrática").*
>
> *Por ello, la policía y otras autoridades con funciones coercitivas que utilicen drones deben asegurarse de que existen unos fundamentos jurídicos sólidos para el tratamiento de los datos personales.*
>
> *Los drones solo se deben utilizar cuando se ofrece una demostración concreta de su necesidad y su pertinencia para los fines concretos perseguidos. A*

[22] Vid. De interés el informe jurídico de la AEPD, sobre drones https://www.aepd.es/sites/default/files/2019-09/informe-juridico-rgpd-drones.pdf

este respecto, el Grupo de trabajo del artículo 29 llama la atención sobre su Dictamen 01/2014 sobre la aplicación de los conceptos de necesidad y proporcionalidad y la protección de datos en el sector de los organismos con funciones coercitivas.

Las autoridades mencionadas deberán justificar por qué los instrumentos que tienen a su disposición y por qué alternativas menos invasivas no alcanzarían ese fin (a este fin se podrá prever y exigir una evaluación previa por las Autoridades de Protección de Datos si las prácticas nacionales apoyan ese tipo de evaluaciones).

Además, cuando las autoridades con funciones coercitivas traten datos recogidos por drones sobre delitos civiles, deberán cumplir los requisitos previstos en la Directiva. En particular, estos usos de los drones se deben restringir a los casos en los que el tratamiento es necesario para proteger el interés vital del interesado o para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento o a un tercero a quien se comuniquen los datos.

Una vez establecida la necesidad de drones con fines policiales o coercitivos, de conformidad con el artículo 52, apartado 1, de la Carta y con el artículo 8 del CEDH, su uso deberá ajustarse al principio de proporcionalidad y cumplir los requisitos específicos de la protección de datos: no deberá ir más allá de la necesidad de cumplir el objetivo legítimo perseguido.

En este contexto, se han de aplicar los principios definidos en el Convenio nº 108 del Consejo de Europa y la Recomendación nº R (87) 15 del Comité de Ministros del Consejo de Europa a los Estados miembros por la que se regula el uso de datos personales en el ámbito policial, adoptada el 17 de septiembre de 1987, así como los principios pertinentes de la Decisión Marco sobre la protección de datos.

Además, el Grupo de trabajo del artículo 29 recuerda que los servicios gubernamentales deberán realizar el tratamiento de datos mediante drones para los fines establecidos en la legislación pertinente y que los datos no se deberán utilizar para una vigilancia indiscriminada, el tratamiento masivo de datos, la puesta en común de datos ni la elaboración de perfiles de datos: se deben imponer límites sobre el uso de los drones en las actividades de vigilancia, con el objetivo de evitar que se extiendan y se usen para señalar objetivos basándose en el análisis de los datos. Por consiguiente, los drones solo se deben usar con una serie de propósitos estrictamente enumerados y justificados que se podrían presentar de antemano; en cualquier caso, su uso se debe limitar geográficamente y en el tiempo. Teniendo en cuenta el «efecto inhibitorio» que puede tener el uso de drones en los derechos de libertad de expresión y libertad de reunión, se ha de prestar una atención especial a la necesidad de proteger frente a cualquier tipo de vigilancia, en la medida de lo posible, las manifestaciones públicas y otras reuniones similares.»

En relación con las posibilidades de videograbación también resulta interesante el contenido del Dictamen 4/2004 relativo al tratamiento de datos personales mediante vigilancia por videocámara[23]que en su apartado 6 hace un estudio (algo desfasado a día de hoy, pero no por ello carente de interés) de la videovigi-

[23] Dictamen 4/2004 relativo al tratamiento de datos personales mediante vigilancia por videocámara. WP.89, 11750/02/ES

lancia por videocámara y tratamiento de datos personales en el que sienta las bases y principios que ha plasmado claramente en la normativa vigente (RGPD, DDP, etc.)

El artículo 5 del Real Decreto 1036/2017, de 15 de diciembre, por el que se regula la utilización civil de las aeronaves pilotadas por control remoto, define la aeronave pilotada por control remoto (RPA) como la aeronave no tripulada, dirigida a distancia desde una estación de pilotaje remoto.

Dado que el drone es un elemento móvil, la incorporación al mismo de una videocámara, determina que la grabación por parte de las FCS de imágenes y sonidos en lugares públicos queda comprendida en el ámbito de aplicación de la normativa sobre dispositivos móviles, quedando supeditada la utilización de videocámaras móviles en drones a la autorización administrativa de autoridad que resulte competente.

Como se desprende de la exposición de motivos de la LOV tiene por objeto la regulación del uso, en general, de la grabación de imágenes y sonidos por las FCS.

> *«Ahora es oportuno proceder a la regulación del uso de los medios de grabación de imágenes y sonidos que vienen siendo utilizados por la Fuerzas y Cuerpos de Seguridad, introduciendo las garantías que son precisas para que el ejercicio de los derechos y libertades reconocidos en la Constitución sea máximo y no pueda verse perturbado con un exceso de celo en la defensa de la seguridad pública.»*

Dado lo anterior, creemos que se debe entender de aplicación a los drones todo el articulado relativo a la autorización de videocámaras móviles.

En cuanto a la regulación específica de los drones destaca el Real Decreto 1036/2017, que recoge en su artículo 3 las exclusiones parciales:

> *«....*
>
> *2. A las operaciones de policía atribuidas a las Fuerzas y Cuerpos de Seguridad por la Ley Orgánica 2/1986, de 13 de marzo, y normativa concordante, a las operaciones de aduanas, a las de vigilancia del tránsito viario realizadas directamente por la Dirección General de Tráfico, y a las operaciones realizadas por el Centro Nacional de Inteligencia, únicamente les será de aplicación lo dispuesto en los capítulos I y II, estando en cuanto a la prohibición de sobrevuelo de las instalaciones prevista en el artículo 32 a las funciones que, en relación con dichas instalaciones, correspondan a las Fuerzas y Cuerpos de Seguridad, al Servicio de Vigilancia Aduanera, a la Dirección General de Tráfico, o al Centro Nacional de Inteligencia.*
>
> *Sin perjuicio de la sujeción a las disposiciones a que se refiere el artículo 20.2 y de las obligaciones de notificación de accidentes e incidentes graves conforme a lo previsto en el Reglamento (UE) n.º 996/2010 del Parlamento Europeo y del Consejo, de 20 de octubre de 2010, sobre investigación y prevención de accidentes e incidentes en la aviación civil y por el que se deroga la Directiva 94/56/CE, estas operaciones se realizarán, en todo caso, conforme a las condiciones establecidas en los protocolos adoptados al efecto por el organismo público responsable de la prestación del servicio o realización de la actividad y, en el caso de las funciones de policía atribuidas a las policías locales, en los respectivos Reglamentos de Policías Locales, de modo que no se*

ponga en peligro a otros usuarios del espacio aéreo y a las personas y bienes subyacentes.

Además, las operaciones de los sistemas de aeronaves pilotadas por control remoto (RPAS) en el ejercicio de estas actividades se ajustarán a lo establecido por el organismo público responsable de la prestación del servicio o realización de la actividad que, en todo caso, será responsable de

a) Autorizar la operación.

b) Establecer los requisitos que garanticen que los pilotos remotos y, en su caso, los observadores, cuentan con la cualificación adecuada para realizar las operaciones en condiciones de seguridad que, en todo caso, deberán respetar los mínimos establecidos en los artículos 33.1 y 38.

c) Asegurarse de que la operación puede realizarse en condiciones de seguridad y cumple el resto de los requisitos exigibles conforme a lo previsto en este apartado.

Calificación de las cámaras incorporadas a los drones a los efectos de determinar el procedimiento de autorización.»

En correlación con la normativa expuesta, solo son de aplicación a los drones en funciones de policía la supervisión de AESA en cuanto a las disposiciones generales del capítulo I y los requisitos de los sistemas RPAS del capítulo II, quedando excluidas la aplicación de las normas de los capítulos III, IV, V o VI, que regulan, respectivamente, las condiciones para la utilización del espacio aéreo, los requisitos de las operaciones, sobre los pilotos y la habilitación para el ejercicio de operaciones aéreas especializadas.

Sin olvidar que, en base a lo requerido por la AEPD, en el caso de zonas autorizadas para el uso de dispositivos móviles en base al peligro o los eventos concretos, pudiera ser necesario también señalizar la zona de operaciones con material que contenga la información legal en materia de protección de datos.

VI. TRATAMIENTO Y CONSERVACIÓN DE DATOS

El artículo 18 de la LOPDP, hace referencia al tratamiento específico y establece un plazo concreto de conservación de las imágenes:

> *«1. Realizada la filmación de acuerdo con los requisitos establecidos en esta Ley Orgánica, si la grabación captara la comisión de hechos que pudieran ser constitutivos de infracciones penales, las Fuerzas y Cuerpos de Seguridad pondrán la cinta o soporte original de las imágenes y sonidos en su integridad, a disposición judicial a la mayor brevedad posible y, en todo caso, en el plazo máximo de setenta y dos horas desde su grabación. De no poder redactarse el atestado en tal plazo, se relatarán verbalmente los hechos a la autoridad judicial, o al Ministerio Fiscal, junto con la entrega de la grabación.*
>
> *2. Si se captaran hechos que pudieran ser constitutivos de infracciones administrativas relacionadas con la seguridad pública, se remitirán al órgano competente, de inmediato, para el inicio del oportuno procedimiento sancionador...»*

Se observa que se mantiene la misma redacción que la recogida en el artículo 7 de la LOV, ya que dispone que, una vez realizada la filmación con los requisitos establecidos, si de la grabación se derivan hechos constitutivos de infracción penal las evidencias digitales (imagen y, en su caso, sonido) se deberán poner en su integridad a disposición de la autoridad judicial, fijándose un plazo máximo de 72 horas. En el supuesto, de que se aprecien hechos constitutivos de infracción administrativa se debe remitir al órgano competente de manera inmediata, no recogiéndose un plazo máximo de remisión.

Está dando algunos problemas de interpretación la expresión del apartado 1 «*pondrán la cinta o soporte original de las imágenes y sonidos en su integridad*», cuestión ésta que debe analizarse desde el prisma de lo que debe entenderse por cita o soporte dentro de ámbito informático donde se almacenan a día de hoy prácticamente la totalidad de la información.

A día de hoy, el concepto de evidencia digital está definido por los Tribunales, los peritos y forenses como cualquier información contenida o transmitida en formato digital de manera que pueda ser utilizada en un juicio.

Las características que la convierten en tal evidencia son la intangibilidad, la posible volatilidad, que puede duplicarse de forma exacta y examinar la copia como si fuera el original, pueden ser localizadas en cualquier soporte y exigen procedimientos forenses especializados para ser examinadas con garantías.

La metodología a emplear pues debe ser correctamente aplicada conforme a la legislación y la jurisprudencia en aras de facilitar las imágenes.

A modo de evidencia de esta cuestión la SAN 5149/2021[24], en su fundamento jurídico sexto señala:

> *«Desde otro punto de vista, la Agencia Española de Protección de Datos, ya dio trámite a la reclamación del recurrente, y resolvió que no existía vulne-*

[24] SAN 5149/2021 - ECLI:ES:AN:2021:5149, de fecha 01/12/2021.

ración de ningún precepto especifico de la LOPD, criterio plenamente compartido por la Sala, por cuanto la captación de imágenes a través de las cámaras instaladas en los acuartelamientos, es legítima, siempre que responda a los fines de cumplimiento de las funciones de velar por el estricto cumplimiento de los deberes de los miembros de la Guardia Civil. Por otro lado, las propias normas internas de la Guardia Civil, contenidas en la Instrucción nº 2, autorizan a hacer copias de imágenes con determinados requisitos (si se hubiera registrado en el documento adecuado y levantado acta, haciendo constar estas circunstancias, pasando las imágenes a otro soporte que quedara almacenado en el acuartelamiento con las debidas medidas de seguridad), y el hecho de que no se hubiera cumplido de firma rigurosa con dichos requisitos, repetimos, no supone una vulneración de la LOPD, sino en todo caso de las normas internas de la Guardia Civil.»

En el apartado segundo no se exige tanta rigurosidad, si bien, si se pretenden usar como elementos de prueba también deberá garantizarse en lo posible el tratamiento que permita su análisis y estudio como tal.

En cuanto al plazo de conservación de las imágenes, se fija en el apartado tercero del artículo 18, que:

.."3. Las grabaciones serán destruidas en el plazo máximo de tres meses desde su captación, salvo que estén relacionadas con infracciones penales o administrativas graves o muy graves en materia de seguridad pública, sujetas a una investigación policial en curso o con un procedimiento judicial o administrativo abierto."

Se observa cómo se pasa de un plazo de conservación obligado de un mes (artículo 7 de la LOV) a un plazo general de conservación con un periodo máximo de tres meses, manteniéndose en los mismos términos el supuesto excepcional de conservación de aquellas grabaciones relacionadas con infracciones penales o administrativas graves o muy graves en materia de seguridad pública, sujetas a una investigación policial en curso o con un procedimiento judicial o administrativo abierto.

Esta cuestión es significativa porque el legislador nos habla de un plazo máximo, pero deja en manos de los responsables el periodo mínimo de conservación. Cuestión ésta debe llevar un ejercicio de ponderación de los derechos en juego tanto en aras de no conservar por más tiempo del necesario como de almacenar estos datos el tiempo mínimo necesario para que se puedan ejercer los derechos por parte de los interesados. Tan perjudicial para los derechos de los ciudadanos resulta ser el mantener los datos por plazos prolongados, como el suprimir o eliminar los datos en plazos que hagan infructuoso el ejercicio de sus derechos.

Como en el resto de los tratamientos de datos, las imágenes y los demás datos derivados de esta actividad deberán ser tratados por los distintos responsables con las medidas de seguridad oportunas. Tanto de carácter técnico como aquellas de carácter organizativo necesarias.

En la normativa específica de aplicación, más allá de los principios de reserva y sigilo, y la prohibición de la cesión, salvo en supuestos recogidos legalmente,

no aparecen referencias expresas relativas a la custodia de las grabaciones por lo que será el responsable el que deba determinar todas estas cuestiones.[25]

Sí son de aplicación las previsiones de la LOPDP y de manera subsidiaria las disposiciones del Reglamento de Protección de Datos.

En cuanto al acceso a las imágenes de las cámaras por cuenta de tercero distinto del responsable de tratamiento deberá estar regulado conforme a los artículos 30 y 31 de la LOPDP.

Es decir, cuando la una operación de tratamiento vaya a ser llevada a cabo por cuenta de un responsable del tratamiento, este recurrirá únicamente a encargados que ofrezcan garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento sea conforme con los requisitos de la LOPDP y se garantice la protección de los derechos del interesado.

Estos encargados podrán ser personas físicas o jurídicas, de naturaleza privada o pública y no podrán recurrir a otro encargado sin la autorización previa por escrito del responsable.

El tratamiento por medio de un encargado se regirá por un contrato, convenio u otro instrumento jurídico que corresponda, por escrito, incluyendo la posibilidad del formato electrónico, concluido con arreglo al Derecho de la Unión Europea o a la legislación española.

Este instrumento jurídico vinculará al encargado con el responsable y fijará el objeto y la duración del tratamiento, su naturaleza y finalidad, el tipo de datos personales y categorías de interesados, así como las obligaciones y derechos del responsable y estipulará la siguiente:

a) Actuar únicamente siguiendo las instrucciones del responsable del tratamiento.

---

[25] El Decreto catalán regula en su Artículo 14 relativo a la custodia de las grabaciones las obligaciones del responsable de custodia de grabaciones:

«14.*1 El responsable de operaciones de grabación, con la periodicidad que se fije en la resolución de autorización en el caso de los dispositivos fijos, e inmediatamente después de finalizarla, en el caso de las efectuadas por equipos móviles, remitirá los soportes originales al responsable de su custodia, sin extraer ninguna copia ni realizar manipulaciones de ninguna clase.*

14.2 Serán responsables de la custodia de las grabaciones:

Respecto de las obtenidas con videocámaras fijas, la persona que se determine en la resolución de autorización, de acuerdo con lo establecido en el artículo 9.1 de este reglamento.

Respecto de las obtenidas con equipos móviles, el jefe de la región policial correspondiente en los territorios de despliegue de la policía de la Generalidad-mozos de escuadra, o el jefe de división, si las ha realizado este cuerpo policial, y el jefe superior de la policía local correspondiente, de las realizadas por ésta.

Los responsables de la custodia de las grabaciones y todas las personas que hayan tenido acceso a ellas están obligados a guardar reserva sobre éstas.

14.3 Nadie podrá realizar ninguna clase de manipulación de los soportes originales de las grabaciones que altere las imágenes y los sonidos recogidos. Sólo se podrán copiar, por orden del responsable de la custodia de las grabaciones, las imágenes y los sonidos del soporte original en el caso previsto en el artículo siguiente, y siempre respetando las siguientes condiciones:

a) Que la copia se realice de punto a punto del soporte original, sin interrupciones, cortes ni inclusiones de imágenes o sonidos intermedios.

b) Que en el punto de inicio y de final de la copia se indique el momento al cual corresponde en el soporte original.

c) Que la copia sea siempre conjunta de imagen y de sonido, en su caso, tal y como figura en el soporte original.

d) Que cada copia se numere de forma independiente y se indique su soporte original.»

b) Garantizar, a través del instrumento o sistema oportuno, que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación profesional de secreto o confidencialidad.
c) Asistir al responsable del tratamiento por cualquier medio adecuado para garantizar el cumplimiento de las disposiciones sobre los derechos del interesado.
d) Suprimir o devolver, a elección del responsable del tratamiento, todos los datos personales al responsable del tratamiento, una vez finalice la prestación de los servicios de tratamiento, así como suprimir las copias existentes, a menos que el Derecho de la Unión Europea o la legislación española requieran la conservación de los datos personales.
e) Poner a disposición del responsable del tratamiento toda la información necesaria para demostrar el cumplimiento de estas obligaciones.
f) Respetar las condiciones indicadas en este apartado y en el apartado 2 para contratar a otro encargado del tratamiento.

Si un encargado del tratamiento determinase los fines y medios de dicho tratamiento, infringiendo la LOPDP, será considerado responsable con respecto a ese tratamiento.

VII. SEÑALIZACIÓN

La LOPDP no recoge en su articulado los derechos de los interesados con respecto a la videovigilancia, pudiendo entenderse de aplicación el artículo 9 de la LOV y, en lo que resulte oportuno, los artículos 22.4 y 89 de la LOPDGDD:

> *«Artículo 9. Derechos de los interesados.*
>
> *1. El público será informado de manera clara y permanente de la existencia de videocámaras fijas, sin especificar su emplazamiento, y de la autoridad responsable.*
>
> *2. Toda persona interesada podrá ejercer los derechos de acceso y cancelación de las grabaciones en que razonablemente considere que figura. No obstante, el ejercicio de estos derechos podrá ser denegado por quien custodie las imágenes y sonidos, en función de los peligros que pudieran derivarse para la defensa del Estado, la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que se estén realizando.*
>
> *«Artículo 22. Tratamientos con fines de videovigilancia.»*
>
> *4. El deber de información previsto en el artículo 12 del Reglamento (UE) 2016/679 se entenderá cumplido mediante la colocación de un dispositivo informativo en lugar suficientemente visible identificando, al menos, la existencia del tratamiento, la identidad del responsable y la posibilidad de ejercitar los derechos previstos en los artículos 15 a 22 del Reglamento (UE) 2016/679. También podrá incluirse en el dispositivo informativo un código de conexión o dirección de internet a esta información. En todo caso, el responsable del tratamiento deberá mantener a disposición de los afectados la información a la que se refiere el citado reglamento.»*

De la referida redacción, cabe entender que existe una obligación de información a la ciudadanía con respecto a las videocámaras fijas, no mencionándose nada de las móviles. Respecto al derecho de información reciente jurisprudencia del TS establece:

> *«... que no se vulnera el derecho de información de un funcionario cuando este ya conocía la instalación de cámaras de video-vigilancia, y ello, aunque no haya sido advertido de que las imágenes se podían utilizar en un procedimiento disciplinario.*
>
> *Así detectó conductas tendentes a eludir los controles sobre el cumplimiento horario de los funcionarios, intentando sortear dicho control en lo relativo al fichaje a la entrada o salida, y también sustituyendo en esa función a otro funcionario...»*

Este distintivo debe exhibirse en lugar visible, y como mínimo, en los accesos a las zonas vigiladas, ya sean interiores o exteriores. En caso de que el espacio video vigilado disponga de varios accesos deberá disponerse de dicho distintivo de zona video vigilada en cada uno de ellos.

El distintivo debe informar de:

- La existencia del tratamiento.
- La identidad del responsable de tratamiento o del sistema de videovigilancia, y la dirección del mismo.
- La posibilidad de ejercicio de los derechos reconocidos en los artículos 20 a 25 de la LOPDP.

- Dónde obtener más información sobre tratamiento de datos personales.
- Asimismo, también se pondrá a disposición de los interesados en resto de información que debe facilitarse a los afectados en cumplimiento del derecho en el RGPD.

El Tribunal Supremo determina el alcance del deber de información de la instalación de cámaras, señalando que no alcanza a exigir una concreta y específica previsión sobre el posterior uso a los funcionarios públicos afectado, es decir, sobre la finalidad específica de su utilización, en el caso de eventuales procedimientos disciplinarios. Según los magistrados, el derecho de información no alcanza a especificar la finalidad que se persigue con la captación de imagen que realizan las cámaras de videovigilancia instaladas. Del mismo modo, en cuanto al consentimiento, no se necesita el consentimiento expreso del trabajador para el tratamiento de las imágenes que han sido obtenidas a través de las cámaras instaladas en la empresa con la finalidad de seguridad o control laboral, porque el consentimiento se entiende implícito con la aceptación del contrato de trabajo, que implica reconocimiento del poder de dirección del empresario.

Estas conclusiones derivan de diversas sentencias del Tribunal de Justicia de la Unión Europea y del Tribunal Europeo de Derechos Humanos cuyas conclusiones han incorporado en sus decisiones en varias ocasiones el Tribunal Supremo Español.

Resultan muy clarificadoras las Sentencias López Ribalda y otros contra España (Demandas nº 1874/13 y 8567/13), STEDH (Gran Sala) de 17 de octubre de 2019 (números 1874/13 y 8567/13) (asunto López Ribalda II), la STEDH (Gran Sala) Caso Barbulescu contra Rumania. Sentencia de 5 septiembre 2017, la Sentencia 39/2016, de 3 de marzo de 2016. Recurso de amparo 7222-2013 del Tribunal Constitucional y la reciente STS 3115/2021, de 21 de julio de 2021.[26]

Se adjuntan nuevamente para mejor referencia los modelos de cartelería con la información que se requiere para la señalización de las zonas videovigiladas.

[26] STS 3115/2021 - ECLI:ES:TS:2021:3115

Y en el caso de drones en un espacio determinado sería pertinente la publicidad de manera similar al cuadro que se reproduce a continuación, completado con la información mínima apuntada:

VIII. SUPUESTOS ESPECIALES: INFRAESTRUCTURAS CRÍTICAS

En lo relativo a la protección de las infraestructuras estratégicas, cabe mencionar que el Plan Nacional de Protección de las Infraestructuras Críticas establece los criterios y las directrices precisas para movilizar, en cumplimiento de la Ley 8/2011, por las que se establecen medidas para la protección de infraestructuras críticas, las capacidades operativas de las autoridades competentes y de los operadores críticos responsables, articulando las medidas y las respuestas integradas necesarias para asegurar la protección permanente, actualizada y homogénea del Sistema de Protección de Infraestructuras Críticas frente a amenazas de carácter deliberado.

Las infraestructuras críticas objeto de protección conforme a lo establecido por este Plan se encuentran registradas e incluidas en el Catálogo Nacional de Infraestructuras Estratégicas. El Catálogo contiene la información completa, actualizada, contrastada y sistematizada relativa a cada una de las infraestructuras estratégicas identificadas en el territorio nacional, siendo por tanto un elemento esencial del Sistema PIC. Está depositado en el CNPIC, a quien concierne la custodia, gestión, mantenimiento y actualización continuos.

Por otro lado, resulta de interés diferenciar el concepto de operador crítico, entendiendo como tal las entidades u organismos responsables de las inversiones o del funcionamiento diario de una instalación, red, sistema, o equipo físico o de tecnología de la información designada como infraestructura crítica con arreglo a la Ley 8/2011.

Como se ha expuesto, la instalación de videocámaras en lugares públicos, es competencia exclusiva de las FCS, rigiéndose el tratamiento de dichas imágenes por la legislación específica de protección datos, en lo no aplicable la LOV y el Reglamento LOV, en diferentes aspectos como la adopción de las medidas de seguridad o el registro de actividades de tratamiento.

En el marco de la Seguridad Privada, la LSP, prohíbe la utilización de cámaras o videocámaras con fines de seguridad privada para tomar imágenes de vías públicas salvo en los supuestos y condiciones previstos en su normativa específica, estando pendiente el desarrollo reglamentario ulterior de la norma.

En relación con la LOPDP, el artículo 22 establece los tratamientos con fines de videovigilancia:

> *«las personas físicas o jurídicas, públicas o privadas, podrán llevar a cabo el tratamiento de imágenes a través de sistemas de cámaras o videocámaras con la finalidad de preservar la seguridad de las personas y bienes, así como de sus instalaciones»*, añadiendo que:
>
> *«Solo podrán captarse imágenes de la vía pública en la medida en que resulte imprescindible para la finalidad mencionada en el apartado anterior»*.

No obstante, la referida regulación matiza que:

> *«será posible la captación de la vía pública en una extensión superior cuando fuese necesario para garantizar la seguridad de bienes o instalaciones estratégicos o de infraestructuras vinculadas al transporte, sin que en ningún*

caso pueda suponer la captación de imágenes del interior de un domicilio privado».

De todo lo expuesto, se deduce que, considerando el ordenamiento jurídico vigente, la solicitud de instalación de videocámaras exteriores perimetrales, acogiéndose a lo dispuesto en el artículo 14.4 de la LPIC, exige que la instalación esté identificada como infraestructuras críticas objeto de protección conforme al Catálogo Nacional de Infraestructuras Estratégicas.

IX. RÉGIMEN DISCIPLINARIO

Al conformar un derecho fundamental, nuestro ordenamiento entiende que la vulneración de este bien jurídico protegido debe llevar aparejada una sanción que se ajuste precisamente a dicho concepto.

Como sabemos, el Derecho penal debería ser la última ratio en su aplicación y antes de llegar a dicho grado punitivo, es necesario desarrollar un sistema que garantice la respuesta de la sociedad ante posibles infracciones que no lleguen a constituir conductas penales. Este sería el procedimiento desarrollado que obliga a que en las FCS se consideren infracciones la infracción de lo contenido en las previsiones legales sobre videoviglancia que no constituyan infracción penal.

La exigencia de respuesta disciplinaria prevista la encontramos recogida en el artículo 19 de LOPDP:

> «1. *Sin perjuicio de las responsabilidades penales en las que pudieran incurrir, las infracciones a lo dispuesto en esta Ley Orgánica por los miembros de las Fuerzas y Cuerpos de Seguridad, serán sancionadas con arreglo al régimen disciplinario correspondiente a los infractores y, en su defecto, con sujeción al régimen general de sanciones en materia de protección de datos de carácter personal establecido en esta Ley Orgánica.*
>
> *2. Se considerarán faltas muy graves en el régimen disciplinario de las Fuerzas y Cuerpos de Seguridad del Estado, las siguientes infracciones:*
>
> *a) Alterar o manipular los registros de imágenes y sonidos, siempre que no constituya delito.*
>
> *b) Permitir el acceso de personas no autorizadas a las imágenes y sonidos grabados o utilizar estos para fines distintos de los previstos legalmente.*
>
> *c) Reproducir las imágenes y sonidos para fines distintos de los previstos en esta Ley Orgánica.*
>
> *d) Utilizar los medios técnicos regulados en esta Ley Orgánica para fines distintos de los previstos en la misma.»*

Se recogen las mismas faltas que estableció la disposición adicional 7 de la LOV, la cual incluyó las faltas enumeradas en el régimen disciplinario de las FCSE, siendo consideradas muy graves las enunciada en el artículo 19. 2 de la LOPCS.

Si bien, en este caso, es oportuno señalar que el legislador ha dejado meridianamente claro que estas infracciones de carácter disciplinario lo son, al margen de posibles responsabilidades penales y, en su defecto de ambas, con sujeción a la normativa de protección de datos de carácter personal.

Teniendo en consideración el que el cumplimento del principio *«non bis in ídem»* exige que concurran los presupuestos de identidad de sujeto, fundamento. Si dichos principios no coinciden se podrá proceder en los diversos ámbitos contra los sujetos infractores[27].

---

[27] Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público Art. 31 dispone: *«1. No podrán sancionarse los hechos que lo hayan sido penal o administrativamente, en los casos en que se aprecie identidad del sujeto, hecho y fundamento. 2. Cuando un órgano de la Unión Europea hubiera impuesto una sanción por los mismos hech*os, y siempre que no concurra la identidad de sujeto y fundamento, el órgano competente para resolver deberá *tenerla en cuenta a efectos de graduar la que, en su caso, deba imponer, pudiendo minorarla, sin perjuicio de declarar la comisión de la infracción.»*

CAPÍTULO 5.
PROCEDIMIENTO SANCIONADOR

I. INTRODUCCIÓN

Las vulneraciones de las normas que regulan la protección de los datos personales exige la adopción de medidas correctivas que conlleven no sólo el castigo de sus responsables, sino también la reposición de la situación alterada, el resarcimiento de quienes hayan sido perjudicados y la disuasión frente ulteriores conductas transgresoras. En este sentido el RGPD otorga el derecho a toda persona que haya sufrido daños y perjuicios (materiales o inmateriales) como consecuencia de una infracción del Reglamento, a reclamar una indemnización ante los tribunales competentes al responsable o encargado del tratamiento; y ello sin perjuicio de su derecho a presentar una denuncia ante la Agencia Española de Protección de Datos por dicha infracción.

En el ejercicio de su derecho a la tutela judicial efectiva, las personas físicas pueden ser representadas por organizaciones sin ánimo de lucro activas en el campo de la protección de datos.

Los interesados podrán, como último recurso y en determinadas circunstancias, interponer un recurso contra las violaciones de la legislación en materia de protección de datos ante el Tribunal Europeo de Derechos Humanos.

Como se apuntaba en el primer capítulo del texto, para encauzar correctamente su protección debemos diferenciar el derecho a la protección de datos de aquellos otros con los que, si bien guarda una estrecha relación, se trata de derechos distintos que tienen su propio sistema de protección.

En este sentido se trae de nuevo a colación la Sentencia 292/2000 del Tribunal Constitucional, de 30 de noviembre, que distingue entre el derecho a la intimidad y a la protección de datos personales en los siguientes Fundamentos Jurídicos:

> *«5. ...Este derecho fundamental a la protección de datos, a diferencia del derecho a la intimidad del art. 18.1 C.E., con quien comparte el objetivo de ofrecer una eficaz protección constitucional de la vida privada personal y familiar, atribuye a su titular un haz de facultades que consiste en su mayor parte en el poder jurídico de imponer a terceros la realización u omisión de determinados comportamientos ..... La peculiaridad de este derecho fundamental a la protección de datos respecto de aquel derecho fundamental tan afín como es el de la intimidad radica, pues, en su distinta función, lo que apareja, por consiguiente, que también su objeto y contenido difieran.*
>
> *6. La función del derecho fundamental a la intimidad del art. 18.1 C.E. es la de proteger frente a cualquier invasión que pueda realizarse en aquel ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad (por todas STC 144/1999, de 22 de julio, F.J. 8). En cambio, el derecho fundamental a la protección de datos persigue garantizar a esa persona un poder de*

control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado. En fin, el derecho a la intimidad permite excluir ciertos datos de una persona del conocimiento ajeno, por esta razón..., es decir, el poder de resguardar su vida privada de una publicidad no querida. El derecho a la protección de datos garantiza a los individuos un poder de disposición sobre esos datos....

De ahí la singularidad del derecho a la protección de datos, pues, por un lado, su objeto es más amplio que el del derecho a la intimidad, ya que el derecho fundamental a la protección de datos extiende su garantía no sólo a la intimidad en su dimensión constitucionalmente protegida por el art. 18.1 C.E., sino a lo que en ocasiones este Tribunal ha definido en términos más amplios como esfera de los bienes de la personalidad que pertenecen al ámbito de la vida privada, inextricablemente unidos al respeto de la dignidad personal (STC 170/1987, de 30 de octubre, F.J. 4), como el derecho al honor, citado expresamente en el art. 18.4 C.E., e igualmente, en expresión bien amplia del propio art. 18.4 C.E., al pleno ejercicio de los derechos de la persona.

Pero también el derecho fundamental a la protección de datos posee una segunda peculiaridad que lo distingue de otros, como el derecho a la intimidad personal y familiar del art. 18.1 C.E. Dicha peculiaridad radica en su contenido, ya que a diferencia de este último, que confiere a la persona el poder jurídico de imponer a terceros el deber de abstenerse de toda intromisión en la esfera íntima de la persona y la prohibición de hacer uso de lo así conocido... el derecho a la protección de datos atribuye a su titular un haz de facultades consistente en diversos poderes jurídicos cuyo ejercicio impone a terceros deberes jurídicos, que no se contienen en el derecho fundamental a la intimidad, y que sirven a la capital función que desempeña este derecho fundamental: garantizar a la persona un poder de control sobre sus datos personales, lo que sólo es posible y efectivo imponiendo a terceros los mencionados deberes de hacer. A saber: el derecho a que se requiera el previo consentimiento para la recogida y uso de los datos personales, el derecho a saber y ser informado sobre el destino y uso de esos datos y el derecho a acceder, rectificar y cancelar dichos datos.

En definitiva, el poder de disposición sobre los datos personales....

7. ...el contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso...».

La vinculación o similitud de derechos que se pueden ver afectados por una conducta vulneradora de los mismos, exige determinar con la mayor precisión posible, las circunstancias del hecho, de manera que permita deslindar, conforme al principio de tipicidad, el concreto derecho que ha sido objeto de ataque, por cuanto en muchos casos difieren en su sistema de protección y respuesta sancionadora.

Un ejemplo de esta concurrencia de infracciones penales y administrativas lo podemos observar en el uso de las nuevas tecnologías de la información y la comunicación, en cuya esfera no sólo es constante y progresiva la comisión de in-

fracciones en materia de protección de datos, sino también para cometer diferentes delitos[1] como estafas, acoso, amenazas, coacciones, delitos sexuales, descubrimiento y revelación de secretos, etc.

Nuestro ordenamiento jurídico ha establecido mecanismos que permiten incardinar una conducta en un concreto procedimiento sancionador tales como: el concurso de normas, el principio «non bis in ídem», o la vinculación del procedimiento administrativo sancionador al penal; a todos ellos haremos referencia a lo largo del presente capítulo.

Comenzaremos por dos principios independientes entre sí pero complementarios y necesarios, dependiendo uno del otro, así previamente se ha de delimitar la norma aplicable entre las concurrentes a través del principio «non bis in ídem» y tras ello, determinar la responsabilidad del sujeto activo por medio del principio de culpabilidad, configurado como un límite del *«ius puniendi»* del Estado, puesto que para imponer una pena o sanción a un sujeto, debe ser responsable del hecho que motiva su imposición.

Ateniéndonos al régimen sancionador configurado por la normativa sobre protección de datos, nos podemos preguntar si un hecho puede ser constitutivo de varias sanciones (penal, administrativa y disciplinaria).

Para determinar los distintos supuestos en los que pueden concurrir diversas sanciones por un mismo hecho, debemos tener en cuenta el «principio non bis in ídem», se trata de un principio constitucionalizado e incluido indirectamente en el artículo 25 de nuestra Carta Magna, siendo una manifestación del principio de legalidad, por lo que tiene la consideración de derecho fundamental, cuyo quebranto permite interponer recurso de amparo ante el Tribunal Constitucional, a su vez es un principio general del derecho, recogido en el artículo 31.1 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (en adelante LRJSP): *«No podrán sancionarse los hechos que lo hayan sido penal o administrativamente, en los casos en que se aprecie identidad del sujeto, hecho y fundamento».*

Pero no se trata de un principio absoluto, ya que el mismo tiene sus excepciones estando justificada una doble sanción administrativa y penal cuando las normas aplicables persiguen intereses jurídicos distintos. Así, por ejemplo, un funcionario público que haya sido sancionado en el ámbito penal puede ser sancionado disciplinaria o administrativamente, no infringiendo esta segunda sanción el principio *«non bis in ídem»* puesto que se protegen intereses jurídicamente distintos.

Este principio requiere para su aplicación la concurrencia de dos requisitos:

- Por un lado, una triple identidad de sujeto, hecho y fundamento jurídico.
- Por otro lado, la ausencia de una relación de sujeción especial entre el sujeto infractor y la Administración Pública con relación al hecho infractor, pues de lo contrario, de existir esta relación especial, podría estar justificada una compatibilidad de sanciones administrativa y penal.

[1] Vid. en extenso: https://www.aepd.es/sites/default/files/2019-11/guia-proteccion-datos-y-prevencion-de-delitos.pdf

En este último supuesto, el Tribunal Supremo en numerosas sentencias, v.g. sentencias de 19 de noviembre de 2008 y 27 de febrero de 2009, explica que:

> *«... en el tipo disciplinario consistente en la realización de "cualquier conducta constitutiva de delito doloso" el fundamento de la sanción es procurar la irreprochabilidad penal de los funcionarios, en cuanto interés legítimo y propio de la Administración Pública, y para que esta satisfaga adecuadamente los intereses generales a cuyo servicio viene constitucionalmente obligada»*. De este modo si, en los delitos por los que es condenado el funcionario, su condición de tal no es elemento determinante de los tipos penales, no se puede entender infringido el principio non bis in ídem, siempre que resulte claro que el bien jurídico protegido por el delito es otro, como puede ser la libertad de las personas o la integridad física.

Por otro lado, la Sentencia del Tribunal Supremo de 3 de noviembre de 2014, en resolución del recurso de casación 832/2013, en el fundamento jurídico cuarto, precisa que: *«... lo que se garantiza con la sanción disciplinaria es que el servicio a la sociedad se preste en las condiciones adecuadas por los funcionarios públicos (por todas, Sentencias 94/1986, de 8 de julio, 98/1989, de 1 de junio, o 154/1990, de 15 de octubre)».*

El principio *«non bis in ídem»* tiene una doble dimensión, tal y como explica la STC 188/2005, de 7 de Julio:

- La Material o sustantiva, que impide sancionar al mismo sujeto, en más de una ocasión por el mismo hecho con el mismo fundamento, para evitar una reacción punitiva desproporcionada.
- La procesal o formal, que proscribe la duplicidad de procedimientos sancionadores en caso de que exista una triple identidad de sujeto, hecho y fundamento, y que tiene como primera concreción la regla de la preferencia o precedencia de la autoridad judicial penal sobre la Administración respecto de su actuación en materia sancionadora en aquellos casos en los que los hechos a sancionar puedan ser, no solo constitutivos de infracción administrativa, sino también delito o falta según el Código Penal.

La subordinación del procedimiento administrativo al penal, se establece en diversos preceptos de nuestro ordenamiento jurídico, como por ejemplo: en el artículo 77.4 de la Ley 39/2015, de 1 octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (LPACAP), en los arts. 38.4 y 45 de la Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana, o en el artículo 38.1 de la Ley 19/2007, de 11 julio contra la Violencia, el Racismo, la Xenofobia y la Intolerancia en el Deporte.

Por tanto, será necesario determinar si tanto en el procedimiento penal, como en el procedimiento sancionador existe identidad total, o, por el contrario, existe algún elemento novedoso que excluya la aplicación del citado principio.

Ejemplos:

- Sanción de la AEPD a Google:

«La Agencia Española de Protección de Datos (en adelante, AEPD) abrió un procedimiento sancionador en 2010 a Google por captar y almacenar datos personales, mientras procedía a confeccionar el GOOGLE STREET VIEW (es una prestación de Google Maps y de Google Earth que da panorámicas a nivel de calle, permitiendo a los usuarios ver partes de las ciudades seleccionadas), de manera que de forma aleatoria captó una serie de datos personales o privados sin consentimiento de sus titulares, datos que posteriormente no fueron destruidos sino almacenados y cedidos a terceros, a pesar de que Google atribuye dichas circunstancias a errores de tipo técnico.

Entre otras cosas, Google recolectó direcciones de correo electrónico, códigos de usuario y contraseñas que dan acceso a esas cuentas de correo, direcciones IP, direcciones MAC de los routers y de los dispositivos conectados a los mismos, e identificadores de redes inalámbricas (los SSID con los que denominamos a nuestras redes WiFi) asociadas al nombre y apellidos de sus responsables. No quedando constatado que Google tratase datos especialmente protegidos a través de estos sistemas.

Se trata de una captación de datos personales casual como consecuencia de una actividad permitida administrativamente. Sin embargo, el hecho de que dichos datos fueran almacenados y cedidos a su vez a terceros (en este caso se trata de una trasferencia internacional de datos a compañías situadas en U.S.A) sin autorización de sus propietarios, hace que esta ulterior conducta se haya traducido en una violación de los datos personales de los usuarios por medio de las redes wifi, datos de los usuarios tales como contraseñas personales, direcciones de correo electrónico –con nombre y apellidos-, mensajes asociados a dichas cuentas y servicios de mensajería, u otros datos que puedan servir para acceder a datos que vulneren la privacidad de los propios afectados.

Si a esto le unimos el supuesto hecho sobre la transferencia internacional de los mismos, sin observar las garantías previstas en la Ley Orgánica de Protección de Datos, el caso aún se vuelve más grave, y más si tenemos en cuenta que no solo se produjo dicha cesión, sino también el almacenamiento de dichos datos, sin consentimiento de sus titulares.

El proceder de la compañía sobre la que recae el procedimiento sancionador supone una violación flagrante de los derechos fundamentales reconocidos en el art. 18.1 y 4 C.E, ya que el artículo 18 de la Constitución, garantiza el Derecho al honor, la intimidad personal y familiar, y la propia imagen. Al respecto, el Tribunal Constitucional ha tenido la ocasión de advertir, en numerosas ocasiones, «que el derecho a la intimidad personal, consagrado en el artículo 18.1 CE, se configura como un derecho fundamental estrictamente vinculado a la propia personalidad y que deriva, sin ningún género de dudas, de la dignidad de la persona que el artículo 10.1 CE reconoce» (Tribunal Constitucional. Sala Segunda. Sentencia núm. 202/1999 de 8 de noviembre RTC/1999/202).

Pero más concretamente, el derecho fundamental reconocido en el art. 18.4 C.E. es el que resulta vulnerado. Dicho artículo dispone 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». Según reiterada jurisprudencia del Tribunal Constitucional, el artículo 18.4 CE contiene un instituto de garantía de los derechos a la intimidad y al honor, y al pleno disfrute de los restantes derechos de los ciudadanos, y por tanto también, «el derecho fundamental a la protección de datos, entendido como el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento automatizado de datos, lo que la Constitución llama «la informática». (STC 290/2000 de 30 de noviembre, en su Fundamento7º; STC 143/1994, de 9 de mayo en su Fundamento 7º; STC 11/1998 de 13 de enero, en su Fundamento 4º).

La configuración constitucional y legal del derecho fundamental a la protección de datos (en concreto a través de la ley Orgánica de Protección de Datos) confiere a su titular un haz de facultades para garantizar su protección, y le otorga peculiaridades en su contenido, que lo distingue de otros, puesto que confiere a su titular una serie de facultades consistentes en imponer a terceros, determinados deberes jurídicos, que por ejemplo, no contiene el derecho fundamental a la intimidad, es decir, «garantiza a la persona un poder de control sobre sus datos personales», lo que solo es posible y efectivo imponiendo a terceros determinados deberes de hacer (a saber: el derecho a que se requiera el previo consentimiento para la recogida y uso de los datos personales, el derecho a saber y ser informado sobre el destino y uso de los datos, y el derecho a acceder, rectificar y cancelar dichos datos).

Para evitar este tipo de intromisiones, la LOPD otorga a la Agencia Española de Protección de Datos un carácter tuitivo y preventivo de tales derechos, para asegurar, mediante su ejercicio, la salvaguardia y garantía del derecho fundamental a la protección de datos personales en relación con los límites, al uso de la informática.

La Agencia Española de Protección de Datos, tras finalizar las actuaciones previas de inspección dio traslado del informe final de la inspección al Juzgado de Instrucción nº 45 de Madrid, incoando procedimiento sancionador contra la citada empresa, quedando suspendido hasta resolución del procedimiento judicial penal, que se había abierto al respecto, por presuntos «delitos informáticos» (término impreciso, usado por el citado Juzgado en la providencia por la que en su día se citaba a declarar como imputado, al representante legal de Google en España).

El Ministerio Fiscal decidió archivar la investigación por considerar que «el carácter aleatorio, indiscriminado y fragmentario de la técnica utilizada por los automóviles de Google "Street View", impide que se haya obtenido información que, "per se" suponga el descubrimiento de secretos o la vulneración de la intimidad que exige el tipo penal».

Tras dictarse auto por el que se acuerda el sobreseimiento provisional y archivo de las diligencias previas abiertas por el citado Juzgado, la AEPD reanudó el procedimiento administrativo, desembocando en resolución sancionadora dictada en 2017 a Google con 300.000€, porque considera que: «"Google captó y almacenó sin consentimiento datos personales de los ciudadanos procedentes de redes inalámbricas a través de los vehículos empleados en su proyecto Street View ...", vulnerando con ello el artículo 6.1 de la anterior Ley

15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal., puesto que el tratamiento de los datos de carácter personal requiere el «consentimiento inequívoco del afectado, salvo determinadas excepciones no aplicables en este caso concreto».

- Sanción disciplinaria a un miembros de las FCSE[2]:

Sevilla

Interior sanciona a un policía nacional por revelación de secreto

Estará cuatro meses suspendido de sus funciones por supuestamente usar las bases de datos para contactar con personas relacionadas con hechos delictivos.

Un agente de la Policía Nacional con residencia en la provincia de Sevilla pero que presta servicio fuera de ella ha sido sancionado por el Ministerio de Interior con cuatro meses de suspensión de funciones y una «separación del servicio», por aspectos como una «violación del secreto profesional» al servirse supuestamente de las bases de datos policiales para supuestos contactos con personas relacionadas con hechos delictivos.

En una sentencia emitida el pasado 16 de septiembre y recogida por Europa Press, la Audiencia Nacional analiza un recurso contencioso administrativo interpuesto por un agente de la Policía Nacional, contra una resolución del Ministerio de Interior que le impone una suspensión de funciones durante tres meses, como autor de una falta grave del Régimen Disciplinario del Cuerpo Nacional de Policía por violación del secreto profesional; y dos sanciones de separación del servicio como autor de sendas faltas muy graves, por «falta de colaboración manifiesta con otros miembros de las Fuerzas y Cuerpos de Seguridad, cuando resulte perjudicado gravemente el servicio o se deriven consecuencias graves para la seguridad ciudadana».

Dichas sanciones, según la Audiencia Nacional, derivan de un expediente incoado tras la detención del agente por presuntos delitos de cohecho, revelación de secretos y omisión del deber de perseguir delitos, toda vez que en 2018 fueron archivadas las diligencias judiciales abiertas contra este agente porque no quedó «debidamente justificada la perpetración del delito».

Según el expediente que sostiene las sanciones impuestas, en 2017, el agente «consultó en numerosas ocasiones, y por motivos ajenos a la labor policial, los registros obrantes en la base de datos "Personas", de exclusiva utilización para fines policiales», con relación a una mujer y a varios de sus familiares, «revelando en ocasiones a la anterior el resultado de dichas consultas, a sabiendas de que esa persona había sido detenida por su presunta participación en hechos delictivos, y también que tanto ella como los miembros de su familia consultados seguían dedicándose a actividades ilícitas».

Además, el agente habría contactado con una mujer «de la que sabía que se dedicaba a actividades ilícitas y le comunicó que su marido había participado junto a otras dos personas en un hurto de cuatro robots-aspiradora», indicándole

[2] -Nota de prensa: Andalucía Información 20-11-2020.

que su esposo «no se presentase en ninguna dependencia policial hasta que pudiese comprobar si, tal y como sospechaba, constaba contra él alguna requisitoria policial en las bases de datos corporativas».

El agente llegó a alertar a la mujer de que «existía contra su marido una requisitoria policial activa para que se procediese a su detención; revelándole detalles de la investigación y recomendándole también prudencia para que su marido no resultase identificado en la vía pública, y evitar así su detención», tras lo cual habría orquestado una detención acordada con el cónyuge de la mujer.

Además, a petición de una tercera persona, habría revelado a la misma «la información que había obtenido a partir de sus consultas, comunicándole ella que ese vehículo estaba involucrado en un hecho delictivo, que sus autores eran los que le habían solicitado la información que pudiese figurar con respecto a ese vehículo en las aplicaciones policiales, y que los mismos mantenían ese vehículo oculto en algún lugar para evitar su localización, ante lo que indicó que lo limpiasen para hacer desaparecer cualquier tipo de vestigio que pudiese incriminarles».

Frente a dichas sanciones por parte del Ministerio de Interior, el agente invoca en su recurso contencioso administrativo contra las mismas el principio «non bis in ídem», avisando de que «la incoación del procedimiento disciplinario tiene como objeto exactamente los mismos hechos que constituyeron el de las diligencias previas» promovidas en su contra y después sobreseídas. El archivo de la causa judicial, a su juicio, «debió vincular a la Administración a fin de acordar el archivo del expediente disciplinario».

No obstante, la Audiencia Nacional determina que «no se ha vulnerado el principio non bis in ídem porque, ante un auto de sobreseimiento provisional de las diligencias penales, hayan seguido las disciplinarias y culminado con la constatación de la comisión de diversas infracciones administrativas y sus consiguientes sanciones».

La Audiencia Nacional, en ese sentido, sólo estima un aspecto del recurso, mediante el cual la segunda actuación en la que incurrió el agente «en lugar de muy grave se califica como grave, con la consiguiente anulación de la sanción de separación del servicio y su sustitución por la de suspensión de funciones durante un mes».

Así las cosas, una de las dos faltas muy graves atribuidas al agente queda reducida al rango de grave y la sanción de separación del servicio por tal extremo queda sustituida por una suspensión de funciones durante un mes.

Ejemplo[3]:

«Despedida por no respetar la confidencialidad ni la protección de datos.»

La Sala de lo Social del Tribunal Superior de Justicia de Madrid[4], en su sentencia núm. 863/2020, de fecha 30 de septiembre, de 30 de septiembre de 2020, considera válido un despido disciplinario de una trabajadora -embarazada en el momento del despido- por haber infringido la legislación aplicable y las políticas

[3] Ejemplo basado en el artículo escrito por David Molina (Gerente en el área de Derecho Digital IP).

[4] Sentencia núm. 863/2020, de fecha 30 de septiembre, ECLI:ES:TSJM:2020:9709

de confidencialidad y protección de datos de la empresa, al haber substraído numerosa documentación de su empresa.

La sentencia de la Sala de lo Social de dicho tribunal, estima el recurso rectificando la postura del anterior tribunal -que lo había considerado nulo-. Esto implica poder realizar dicho despido cuando antes no era posible, como un considerable ahorro empresarial en el mismo.

En este caso, la violación de la legislación y protocolos en privacidad se produce justo al realizarse el primer despido (que posteriormente sería declarado nulo) cuando se acepta por parte de la empresa que ella pueda copiarse los archivos personales que tiene en su teléfono móvil de empresa. Es entonces cuando vulnera la confidencialidad enviándose todos esos datos personales e información con valor comercial a su cuenta personal y a la de su hermana.

Al sospecharse este hecho, el departamento de Ciberseguridad de la empresa y el Delegado de Protección de Datos lo investigan, tanto para cumplir con la obligación de notificación de brechas de seguridad en 72 horas a la Agencia Española de Protección de Datos y otras obligaciones del Reglamento General de Protección de Datos, como para realizar los esfuerzos razonable para que la información confidencial con valor económico justamente por no ser conocida siga siendo secreta (requisito necesario de la legislación de protección de secretos empresariales para poder protegerlos).

Al encontrar las evidencias necesarias de la infracción se realizaron una serie de comunicaciones legales para intentar contener la fuga de información y se aprovechó para realizar un despido ad cautelam o «despido dentro del despido». Es decir, sabiendo que se ha realizado un claro incumplimiento de la buena fe laboral, de las instrucciones de confidencialidad y de la normativa de protección de datos y sospechando la empresa que el despido inicial podía ser considerado nulo (recordemos que la trabajadora estaba embarazada) se procede a un despido disciplinario. Así ocurrió inicialmente y la empresa necesitó recurrir al Tribunal Superior de Justicia de Madrid.

Además, también hay una clara conclusión para los trabajadores. Si esta directiva de marketing no hubiera incumplido la legislación y la normativa de la empresa de protección de datos y de la información confidencial, su empresa no hubiera podido despedirla y le debería de abonar los salarios de tramitación (su salario entre el despido y su reincorporación); ahora sí puede despedirla y sin necesidad de indemnizarla ni de pagar los salarios de tramitación.

Dicho Tribunal entiende que:

> *«(...) el hecho de que los trabajadores desde su puesto de trabajo puedan y deban acceder a las bases de datos de la empresa para el desempeño de sus funciones, no supone un permiso para disponer particularmente de tales datos, por lo que en absoluto pueden copiarlos, enviarlos o utilizarlos en su propio beneficio, y precisamente en esa confianza los trabajadores prestan sus servicios para las empresas, con el deber de confidencialidad y lealtad, que en este caso se ha vulnerado de forma flagrante y con engaño, ya que, con la excusa de sacar del ordenador de la empresa que tenía a su disposición, archivos personales, lo que hizo fue autoenviarse a su correo privado toda la documentación que consta acreditado, sin que ello fuera permitido por la empresa».*

En los ejemplos anteriores, vemos como la calificación jurídica de un hecho, aparentemente común, como es la revelación de un secreto, puede tener diferentes consecuencias en función del tipo que le sea aplicable, lo que se valorará en relación con las circunstancias que concurran en cada supuesto.

Un elemento esencial para determinar la conducta infractora en materia de protección de datos es el deber de confidencialidad en el tratamiento de datos personales, para lo cual el encargado del tratamiento habrá de garantizar que las personas autorizadas para tratar dichos datos, se deben haber comprometido de forma expresa a respetar la confidencialidad o, estar sujetas a una obligación de confidencialidad de naturaleza estatutaria.

El deber de confidencialidad se encontraría recogido en las siguientes normas:

- Reglamento (UE) 2016/679, artículo 5

> *«1. Los datos personales serán:*
> *(...)*
> *f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas ("integridad y confidencialidad").»*

- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

> *«Artículo 5. Deber de confidencialidad.*
> *1. Los responsables y encargados del tratamiento de datos, así como todas las personas que intervengan en cualquier fase de este estarán sujetas al deber de confidencialidad al que se refiere el artículo 5.1.f) del Reglamento (UE) 2016/679.*
> *2. La obligación general señalada en el apartado anterior será complementaria de los deberes de secreto profesional de conformidad con su normativa aplicable.*
> *3. Las obligaciones establecidas en los apartados anteriores se mantendrán aun cuando hubiese finalizado la relación del obligado con el responsable o encargado del tratamiento».*

La confidencialidad se enmarca dentro de un deber más amplio y del que forma parte, cual es el deber de secreto, que en sí, trata de salvaguardar o tutelar el derecho de las personas a mantener la privacidad de sus datos de carácter personal y en definitiva el poder de control o disposición sobre sus datos. Este deber de secreto está lógicamente relacionado con el secreto profesional, tiene la misma fundamentación jurídica, pero el deber de secreto de la LOPD se refiere al ámbito estricto del tratamiento de los datos personales, en el que el responsable del fichero y, cualquier persona que intervenga en el tratamiento, está obligado a mantener la confidencialidad de los datos personales y no pueda revelar ni dar a conocer su contenido.

El deber de secreto tal y como viene declarando la Audiencia Nacional, entre otras en su Sentencia de 14 de septiembre de 2001 (recaída en el recurso nº 196/2000) resulta esencial en las sociedades actuales cada vez más complejas, en las que los avances de la técnica sitúan a la persona en zonas de riesgo para la protección de derechos fundamentales, como la intimidad o el derecho a la protección de los datos que recoge el artículo 18.4 de la Constitución Española.

El deber de secreto lo encontramos regulado en los siguientes preceptos:

- Ley Orgánica 2/1986, de 13 marzo, de Fuerzas y Cuerpos de Seguridad, artículo 5:

> *«Son principios básicos de actuación de los miembros de las Fuerzas y Cuerpos de Seguridad los siguientes:*
> *(...)*
> *5. Secreto profesional.*
> *Deberán guardar riguroso secreto respecto a todas las informaciones que conozcan por razón o con ocasión del desempeño de sus funciones...».*

- Ley Orgánica 4/2010, de 20 de mayo, del Régimen disciplinario del Cuerpo Nacional de Policía.

> *«Artículo 7. Faltas muy graves.*
> *Son faltas muy graves:*
> *(...)*
> *h) La violación del secreto profesional cuando perjudique el desarrollo de la labor policial, a cualquier ciudadano o a las entidades con personalidad jurídica».*

- Ley Orgánica 12/2007, de 22 de octubre, del régimen disciplinario de la Guardia Civil.

> *Artículo 7. Faltas muy graves.*
> *Son faltas muy graves, siempre que no constituyan delito:*
> *(...)*
> *17. Violar el secreto profesional cuando afecte a la defensa nacional o a la seguridad ciudadana, perjudique el desarrollo de la labor policial o cause daños a personas físicas o jurídicas, públicas o privadas.*

- 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, art. 30.3 el encargado del tratamiento deberá:

> *«b) Garantizar, a través del instrumento o sistema oportuno, que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación profesional de secreto o confidencialidad».*

- Código Penal, Titulo X, Capítulo I. Del descubrimiento y revelación de secretos
  Donde debe destacarse el artículo 197.2 CP que castiga a quien se apodere, utilice o modifique sin autorización datos reservados de carácter personal o familiar que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos o en cualquier otro tipo de archivo público o privado. Estableciéndose tipos agravados en atención a:

  - Si difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas.
  - Se cometan por las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros.

En el artículo 199 CP, se castiga a quien revele secretos ajenos, de los que tenga conocimiento por razón de su oficio o sus relaciones laborales y al profesional que, con incumplimiento de su obligación de sigilo o reserva, divulgue los secretos de otra persona.

En correspondencia con el principio de culpabilidad, artículo 28.1 de la Ley 40/2015 de Régimen Jurídico del Sector Público dispone que:

> *«Sólo podrán ser sancionadas por hechos constitutivos de infracción administrativa las personas físicas y jurídicas, así como, cuando una Ley les reconozca capacidad de obrar, los grupos de afectados, las uniones y entidades sin personalidad jurídica y los patrimonios independientes o autónomos, que resulten responsables de los mismos a título de dolo o culpa».*

La presunción de inocencia debe regir sin excepciones en el procedimiento sancionador y ha de ser respetada en la imposición de cualesquiera sanciones, pues el ejercicio del «*ius puniendi*» en sus diversas manifestaciones está condicionado al juego de la prueba y a un procedimiento contradictorio en el que puedan defender se las propias posiciones.

En tal sentido, el Tribunal Constitucional en su Sentencia nº 76/1990, de 26/04, considera que el derecho a la presunción de inocencia comporta: «que la sanción esté basada en actos o medios probatorios de cargo o incriminadores de la conducta reprochada; que la carga de la prueba corresponda a quien acusa, sin que nadie esté obligado a probar su propia inocencia; y que cualquier insuficiencia en el resultado de las pruebas practicadas, libremente valorado por el órgano sancionador, debe traducirse en un pronunciamiento absolutorio».

Conforme a este principio, no puede imponerse sanción alguna en razón de la culpabilidad del imputado si no existe una actividad probatoria de cargo, que, en la apreciación de las autoridades u órganos llamados a resolver, destruya esta presunción (TC Auto 3-12-81).

La STS de 27/5/99:

> *«Para la imposición de una sanción y las consecuencias derivadas del ilícito administrativo, no basta que la infracción esté tipificada y sancionada, sino que es necesario que se aprecie en el sujeto infractor el elemento o*

categoría denominado culpabilidad. La culpabilidad es el reproche que se hace a una persona, porque ésta debió haber actuado de modo distinto de cómo lo hizo».

La simple inobservancia para la imposición de sanciones en el derecho administrativo sancionador implicaría dar entrada a la responsabilidad objetiva, excluida de nuestro ordenamiento jurídico por el principio de culpabilidad.

Ejemplo: STS 1153/2021, de 22 de marzo:

«SEGUNDO.- Carlos María , cuyos datos de filiación constan, ...de profesión Policía Nacional, destinado en la Brigada Provincial de Seguridad Ciudadana-Atención al Ciudadano Radiopatrullas de la Jefatura Superior de Policía de Madrid, a la sazón pareja sentimental de Felicidad , valiéndose de su condición de policía nacional y con la intención de conocer datos personales de Jose Ramón , a través de la aplicación Personas de la Dirección General de Policía y utilizando su DNI, efectuó consultas sobre los antecedentes del Señor Jose Ramón entre el 1 de enero de 2014 y el 28 de enero de 2015. Igualmente efectúo consultas en la aplicación Objetos, respecto de los vehículos ....FXQ y sobre el vehículo .... YPZ entre el 5 de febrero de 2014 y el 27 de mayo de 2014

(...)

2. En el caso, se declara probado que el recurrente accedió a un fichero donde constan antecedentes policiales. La conducta no es irrelevante, no solo desde la perspectiva del respeto a las normas que regulan el acceso a esta clase de ficheros, en cuanto rechazan el acceso no autorizado, sino también en consideración a la necesaria protección de la intimidad, pues se trata de ficheros donde se almacenan y se tratan informáticamente numerosos datos que, generalmente, se refieren a aspectos de la privacidad de los ciudadanos que deben ser debidamente protegidos.

Pero lo que aquí se cuestiona es si los hechos son típicos desde la descripción contenida en el artículo 197.2 CP, en el que, como ya hemos dicho, se sanciona al que, sin estar autorizado, acceda por cualquier medio a datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado, y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero.

3. ... de los hechos que se declaran probados se desprende, en primer lugar, que, tal como alega el recurrente, no se aclara a qué datos accedió a través de la aplicación Personas de la Dirección General de Policía. Además, no consta que en los ficheros a los que accedió estuvieran registrados datos relativos al denunciante, por lo que no es posible afirmar que tuvo acceso a datos reservados que puedan valorarse como datos relativos a su intimidad personal o familiar.

Lo que el precepto sanciona no es el acceso no autorizado al fichero, sino el acceso no autorizado al dato. Aún podría cuestionarse si ya integra un dato la verificación de la inexistencia de antecedentes policiales. Pero, en cualquier caso, esa inexistencia, al menos considerada en abstracto, no puede calificarse como un dato sensible equiparable a los que hemos citado más arriba. Y tampoco puede afirmarse que del mero conocimiento de la inexistencia de antecedentes policiales se derive un perjuicio para el afectado.

(...)

4. Ninguno de estos datos, con los elementos conocidos, pueden calificarse como especialmente protegidos o sensibles, por lo que sería preciso establecer que el acusado actuó "en perjuicio" del titular o de un tercero. No se recoge en los hechos probados que la acción haya causado algún perjuicio o que el sujeto tuviera intención de causar tal perjuicio o, al menos, que fuera consciente de su causación. Tampoco se puede deducir de la naturaleza de los datos o de otros elementos suficientemente acreditados que esa fuera su intención o el efecto de la acción, más allá de lo que representa el mero acceso. No es posible vincular un perjuicio a la consulta realizada mediante la aplicación Personas de la Dirección General de Policía, ya que se desconoce a qué datos pudo acceder sin que tampoco conste los que en dicho fichero existen sobre el denunciante.

(...)

En consecuencia, no se aprecia la existencia de perjuicio, ni tampoco un menoscabo relevante de los derechos a la intimidad o a la autodeterminación informática del titular de los datos ni de un tercero, por lo que el motivo se estima, haciendo innecesario el examen de los demás motivos del recurso...».

SUPUESTO PRÁCTICO:

¿Puede la policía evitar por protección de datos que grabes su actuación en la calle?

Como ejemplo significativo, tenemos la información publicada por la AEPD, durante el año 2020, donde tras analizar 165 reclamaciones relacionadas con la captación y/o difusión de la imagen de miembros de las fuerzas y cuerpos de seguridad, en redes sociales y aplicaciones de mensajería; realizadas por particulares, generalmente en el marco de actuaciones llevadas a cabo para verificar el efectivo cumplimiento por parte de los ciudadanos de las medidas adoptadas durante el estado de alarma, prácticamente todas ellas han sido archivadas, al no apreciarse que los tratamientos concretos afectados pudieran vulnerar la normativa de protección de datos.

Con independencia del régimen sancionador previsto en la normativa de protección de datos, la Ley Orgánica 4/2015, de 30 marzo, de protección de la seguridad ciudadana (LOPSC) en su artículo 36. 23 establece:

«El uso no autorizado de imágenes o datos personales o profesionales de autoridades o miembros de las Fuerzas y Cuerpos de Seguridad que pueda poner en peligro la seguridad personal o familiar de los agentes, de las instalaciones protegidas o en riesgo el éxito de una operación, con respeto al derecho fundamental a la información».

El Tribunal Constitucional en su sentencia nº 172/2020, declaró la inconstitucionalidad y nulidad del inciso «no autorizado» del citado artículo, al entender que hay censura previa proscrita por el art. 20.2 CE, cuando la difusión de las imágenes o datos se sometan a un previo examen de su contenido por el poder público, de forma que aquélla (la difusión) solo se pueda realizar si éste «otorga el plácet».

En consecuencia, en dicho artículo se somete a la obtención de autorización administrativa previa la actividad consistente en usar imágenes o datos de las autoridades o miembros de las Fuerzas y Cuerpos de Seguridad, resulta contrario a la interdicción de censura previa (art. 20.2 CE).

No obstante, el art. 36.23, no es inconstitucional siempre que se interpreten en el sentido siguiente:

- El término *«uso»* debe interpretarse en el sentido de que para que pueda apreciarse infracción grave es necesaria la publicación o difusión ilícita, no bastando la mera captación no seguida de publicación o difusión; y el término «imágenes o datos personales o profesionales» comprende también las relativas a la vida privada, elemento este que deberá tomarse en cuenta para determinar si prevalece o no el derecho a la información.
  Así en el extracto de la fundamentación de dicha sentencia:

> *«...el art. 36.23 LOPSC, dado que sujeta a la obtención de autorización administrativa previa la actividad consistente en usar imágenes o datos de las autoridades o miembros de las fuerzas y cuerpos de seguridad, resulta contrario a la interdicción de censura previa ex art. 20.2 CE, de modo que procede declarar la inconstitucionalidad del inciso «no autorizado» de dicho precepto....*
>
> *El "uso" como conducta típica, dado que debe poner en peligro [...] o en riesgo alguno de los bienes jurídicos reseñados en el precepto (la seguridad personal o familiar de los agentes, de las instalaciones protegidas o en riesgo el éxito de una operación), no se realiza con la mera captación o tenencia de "imágenes o datos personales y profesionales". Solo será sancionable, por tanto, el acto de publicar o difundir de algún modo, sea por medios tradicionales o a través de los cauces que ofrecen las tecnologías de la información y comunicación, como redes sociales u otras plataformas análogas, de tal manera que no bastará la mera captación no seguida de publicación o difusión de tales imágenes o datos... cabe concluir que el «uso» a que alude el art. 36.23 CE es aquel que no cuenta con el consentimiento de los titulares de las imágenes o datos difundidos.*
>
> *El elemento del tipo consistente en "poner en peligro [...] o en riesgo" alguno de los bienes jurídicos que indica el precepto no cabe entenderlo por sí solo y de un modo aislado...la intervención administrativa solo "se justifica por la existencia de una amenaza concreta [...] que razonablemente sea susceptible de provocar un perjuicio real para la seguridad ciudadana" (art. 4.3 LOPSC) ....*
>
> *El aplicador deberá afrontar un juicio de ponderación de tal modo que únicamente sean merecedores de sanción quienes realicen este tipo de conductas que supongan un peligro para los bienes jurídicos tutelados como pueden ser la seguridad personal o familiar de los agentes, de las instalaciones protegidas o pongan en riesgo el éxito de una operación... Esta ponderación abordará, al menos, (a) la comprobación de si las imágenes o los datos difundidos pertenecen a la vida privada o se relacionan con la actividad oficial de las autoridades o agentes».*

II. PROCEDIMIENTO SANCIONADOR PREVISTO 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 POR EL QUE SE DEROGA LA DIRECTIVA 95/46/CE (REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS)» -EN ADELANTE REGLAMENTO- Y EN LA «LEY ORGÁNICA 3/2018, DE 5 DE DICIEMBRE, DE PROTECCIÓN DE DATOS PERSONALES Y GARANTÍA DE LOS DERECHOS DIGITALES» (LOPDPGDD)

Dentro del conjunto de normas que de una u otra manera hacen referencia a la protección de los datos personales, nos centraremos en aquellas que contienen una regulación con una incidencia más específica sobre la materia, sin perjuicio de hacer una mención tangencial a otros preceptos que pueden incidir en nuestra actuación profesional.

II.1. Competencia sancionadora

- Concepto de autoridad de control o APD:

Son autoridades públicas independientes que supervisan, mediante los poderes de investigación y correctivos, la aplicación de la legislación sobre protección de datos. Estas ofrecen asesoramiento experto en cuestiones relacionadas con la protección de datos y tramitan reclamaciones presentadas por la violación del Reglamento general de protección de datos y las legislaciones nacionales pertinentes. Cada Estado miembro puede establecer una o varias autoridades de control, en este caso debe disponer por ley de mecanismos que garanticen la participación efectiva de dichas autoridades de control en el mecanismo de coherencia y designar a la autoridad de control que actuará como punto de contacto único de cara a la participación efectiva de dichas autoridades en el citado mecanismo, garantizando así una cooperación rápida y fluida con otras autoridades de control).

En nuestro país, a nivel principal esto recae sobre la Agencia Española de Protección de Datos (en adelante AEPD).

La AEPD es una autoridad administrativa independiente de ámbito estatal, de las previstas en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, con personalidad jurídica y plena capacidad pública y privada, que actúa con plena independencia de los poderes públicos en el ejercicio de sus funciones.

Su denominación oficial, de conformidad con lo establecido en el artículo 109.3 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, será *«Agencia Española de Protección de Datos, Autoridad Administrativa Independiente»* y se relaciona con el Gobierno a través del Ministerio de Justicia.

Ésta tendrá la condición de representante común de las autoridades de protección de datos del Reino de España en el CEPD.

La Agencia, el Consejo General del Poder Judicial (y en lo que sea de su competencia la Unidad de Supervisión y Control de Protección de Datos de la Fiscalía General del Estado) colaborarán en aras del adecuado ejercicio de las respectivas competencias que la Ley Orgánica 6/1985, de 1 julio, del Poder Judicial, les atribuye en materia de protección de datos personales en el ámbito de la Administración de Justicia.

Se rige[5] por lo dispuesto en el RGPD, la LOPDGDD, la LOPDP, su Estatuto[6] y sus disposiciones de desarrollo. Supletoriamente, en cuanto sea compatible con su plena independencia, se regirá por las normas citadas en el artículo 110.1 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

La AEPD elaborará y aprobará su presupuesto y lo remitirá al Gobierno para que sea integrado, con independencia, en los Presupuestos Generales del Estado; el régimen de modificaciones y de vinculación de los créditos de su presupuesto será el establecido en su Estatuto.

Corresponde a la Presidencia de la AEPD autorizar las modificaciones presupuestarias que impliquen hasta un tres por ciento de la cifra inicial de su presupuesto total de gastos, siempre que no se incrementen los créditos para gastos de personal. Las restantes modificaciones que no excedan de un cinco por ciento del presupuesto serán autorizadas por el Ministerio de Hacienda y, en los demás casos, por el Gobierno.

Contará para el cumplimiento de sus fines con las asignaciones que se establezcan con cargo a los Presupuestos Generales del Estado, los bienes y valores que constituyan su patrimonio y los ingresos, ordinarios y extraordinarios derivados del ejercicio de sus actividades, incluidos los derivados del ejercicio de las potestades establecidos en el artículo 58 del RGPD. El resultado positivo de sus ingresos se destinará por la AEPD a la dotación de sus reservas con el fin de garantizar su plena independencia.

El personal al servicio de la Agencia Española de Protección de Datos será funcionario o laboral y se regirá por lo previsto en el texto refundido de la Ley del Estatuto Básico del Empleado Público, aprobado por Real Decreto Legislativo 5/2015, de 30 de octubre, y demás normativa reguladora de los funcionarios públicos y, en su caso, por la normativa laboral.

La Agencia elaborará y aprobará su relación de puestos de trabajo, en el marco de los criterios establecidos por el Ministerio de Hacienda, respetando el límite de gasto de personal establecido en el presupuesto. En dicha relación de puestos de trabajo constarán, en todo caso, aquellos puestos que deban ser desempeñados en exclusiva por funcionarios públicos, por consistir en el ejercicio de las funciones que impliquen la participación directa o indirecta en el ejercicio de potestades públicas y la salvaguarda de los intereses generales del Estado y de las Administraciones Públicas.

Sin perjuicio de las competencias atribuidas al Tribunal de Cuentas, la gestión económico-financiera de la Agencia Española de Protección de Datos estará sometida al control de la Intervención General de la Administración del Estado en

[5] Vid. en extenso: https://www.aepd.es/es/la-agencia/transparencia/informacion-de-caracter-institucional-organizativa-y-de-planificacion/marco-normativo

[6] 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

los términos que establece la Ley 47/2003, de 26 de noviembre, General Presupuestaria.

La Presidencia la dirige, ostenta su representación y dicta sus resoluciones, circulares y directrices. Esta estará auxiliada por un Adjunto en el que podrá delegar sus funciones, a excepción de las relacionadas con los procedimientos en caso de posible vulneración de la normativa de protección de datos, y que la sustituirá en el ejercicio de las mismas en los términos previstos en el Estatuto Orgánico de la Agencia Española de Protección de Datos.

Ambos ejercerán sus funciones con plena independencia y objetividad y no estarán sujetos a instrucción alguna en su desempeño. Les será aplicable la legislación reguladora del ejercicio del alto cargo de la Administración General del Estado.

La Presidencia de la Agencia Española de Protección de Datos y su Adjunto serán nombrados por el Gobierno, a propuesta del Ministerio de Justicia, entre personas de reconocida competencia profesional, en particular en materia de protección de datos.

Dos meses antes de producirse la expiración del mandato o, en el resto de las causas de cese, cuando se haya producido éste, el Ministerio de Justicia ordenará la publicación en el Boletín Oficial del Estado de la convocatoria pública de candidatos.

Previa evaluación del mérito, capacidad, competencia e idoneidad de los candidatos, el Gobierno remitirá al Congreso de los Diputados una propuesta de Presidencia y Adjunto acompañada de un informe justificativo que, tras la celebración de la preceptiva audiencia de los candidatos, deberá ser ratificada por la Comisión de Justicia en votación pública por mayoría de tres quintos de sus miembros en primera votación o, de no alcanzarse ésta, por mayoría absoluta en segunda votación, que se realizará inmediatamente después de la primera. En este último supuesto, los votos favorables deberán proceder de Diputados pertenecientes, al menos, a dos grupos parlamentarios diferentes.

La Presidencia y el Adjunto de la AEPD serán nombrados por el Consejo de Ministros mediante real decreto y su mandato tendrá una duración de cinco años y puede ser renovado para otro período de igual duración.

Solo cesarán antes de la expiración de su mandato, a petición propia o por separación acordada por el Consejo de Ministros, por:

- Incumplimiento grave de sus obligaciones,
- Incapacidad sobrevenida para el ejercicio de su función,
- Incompatibilidad,
- Condena firme por delito doloso.

En los supuestos previstos en las letras a), b) y c) será necesaria la ratificación de la separación por las mayorías parlamentarias previstas para su nombramiento.

Los actos y disposiciones dictados por la Presidencia de la Agencia Española de Protección de Datos ponen fin a la vía administrativa, siendo recurribles, directamente, ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional.

El Consejo Consultivo de la Agencia Española de Protección de Datos, es el órgano colegiado que asesora al Presidente de la AEPD, emite informe sobre las

cuestiones que éste le someta y podrá formular propuestas sobre temas relacionados con las materias de competencia de la AEPD. En este órgano, lamentablemente, no está designado ningún representante del Ministerio del Interior (aunque la AEPD es autoridad de control en todas las normas que afectan específicamente a dicho Departamento) Lo cual, es un aspecto a tener en consideración.

A nivel europeo se encuentran la Comisión Nacional de Protección de Datos de Portugal, Garante italiano, la CNIL en Francia, la Österreichische Datenschutzbehörde en Austria, la Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit en Alemania, etc[7].

Y, en la esfera autonómica, con un marco competencial específico, están constituidas las siguientes autoridades de control:

- La Autoridad Catalana de Protección de Datos
- La Agencia Vasca de Protección de Datos
- El Consejo de Transparencia y Protección de Datos de Andalucía.

Las competencias de dichas autoridades autonómicas de control se establecen en el art. 57 de la LOPDGDD, quedando limitadas a los tratamientos que se citan en dicho artículo dentro de la esfera de su territorito.

En este contexto, donde coexisten diversas entidades con funciones complementarias, la autoridad de control principal (a la que corresponda el asunto en base a sus competencias) será la que resuelva las reclamaciones presentadas por los interesados, al ostentar la potestad sancionadora en dicho ámbito.

En todo caso, contra las decisiones adoptadas por la autoridad de control, toda persona física o jurídica tendrá derecho a obtener la tutela judicial efectiva, ello sin perjuicio de cualquier otro recurso administrativo o extrajudicial que fuere procedente.

En el marco de sus respectivas competencias, todas las autoridades de control de nuestro país, se rigen, dentro del ámbito del procedimiento sancionador, por los principios establecidos en la Ley 39/2015, de 1 octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (LPACAP) y en la Ley 40/2015, de 1 octubre, de Régimen Jurídico del Sector Público (LRJSP), conforme a lo dispuesto por el artículo 149.1.18ª de la Constitución, donde se establece como una de las competencias exclusivas del Estado: *«Las bases del régimen jurídico de las Administraciones públicas y del régimen estatutario de sus funcionarios que, en todo caso, garantizarán a los administrados un tratamiento común ante ellas; el procedimiento administrativo común, sin perjuicio de las especialidades derivadas de la organización propia de las Comunidades Autónomas... y el sistema de responsabilidad de todas las Administraciones públicas».*

Por ello al igual que cualquier otro órgano administrativo con competencia sancionadora, las autoridades de control para la iniciación, instrucción y resolución de los correspondientes expedientes sancionadores, deberán atenerse a los principios y garantías que se contienen en dichas normas, y en concreto por lo

[7] Vid. en extenso: https://ec.europa.eu/justice/article-29/structure/data-protection-authorities/index_en.htm

que concierne a nuestra temática, los principios que rigen el procedimiento sancionador recogidos en los artículos 25 a 31 de la LRJSP, que son los siguientes: principio de legalidad, irretroactividad, principio de tipicidad, responsabilidad, proporcionalidad, prescripción y principio non bis in ídem, alguno de los cuales se detallarán más adelante, todo ello en consonancia con los principios constitucionales que se determinan en el artículo 9.3 de nuestra Carta Magna:

> *«La Constitución garantiza el principio de legalidad, la jerarquía normativa, la publicidad de las normas, la irretroactividad de las disposiciones sancionadoras no favorables o restrictivas de derechos individuales, la seguridad jurídica, la responsabilidad y la interdicción de la arbitrariedad de los poderes públicos».*

Sin perjuicio de las potestades atribuidas a las autoridades de control autonómicas, nos centraremos específicamente en la AEPD como autoridad administrativa independiente a nivel estatal, cuyas facultades se establecen en el artículo 47 de la LOPDGDD, en relación con los artículos 57 y 58 del Reglamento.

Los poderes correctivos de los que dispone la Agencia Española de Protección de Datos, como autoridad de control, se establecen en el artículo 58.2 del RGPD. Entre ellos se encuentran:

- La potestad de sancionar con apercibimiento -artículo 58.2.b).
  A título de curiosidad cabe mencionar la interpretación jurisprudencial del apercibimiento conforme a la regulación que establecida el artículo 45.6 de la anterior LOPD, así la Sentencia de la Audiencia Nacional de 29/11/2013, (Rec. 455/2011), Fundamento de Derecho Sexto, sobre el apercibimiento regulado en el citado artículo y a propósito de su naturaleza jurídica advierte que *«no constituye una sanción»* y que se trata de *«medidas correctoras de cesación de la actividad constitutiva de la infracción»* que sustituyen a la sanción.
  La Sentencia entiende que el artículo 45.6 de la LOPD confiere a la AEPD una *«potestad»* diferente de la sancionadora cuyo ejercicio se condiciona a la concurrencia de las especiales circunstancias descritas en el precepto. En congruencia con la naturaleza atribuida al apercibimiento como una alternativa a la sanción cuando, atendidas las circunstancias del caso, el sujeto de la infracción no es merecedor de aquella, y considerando que el objeto del apercibimiento es la imposición de medidas correctoras, la sentencia citada concluye que cuando éstas ya hubieran sido adoptadas, lo procedente en Derecho es acordar el archivo de las actuaciones.
- La potestad de imponer una multa administrativa con arreglo al artículo 83 del RGPD -artículo 58.2 i).
- O la potestad de ordenar al responsable o encargado del tratamiento que las operaciones de tratamiento se ajusten a las disposiciones del RGPD, cuando proceda, de una determinada manera y dentro de un plazo especificado -artículo 58. 2.d).
  Según lo dispuesto en el artículo 83.2 del RGPD, la medida prevista en el artículo 58.2.d) del citado Reglamento es compatible con la sanción consistente en multa administrativa.

Centrándonos en poderes correctivos de la AEPD, estos se concretan en lo siguiente:

- Sancionar a toda persona responsable o encargado del tratamiento con una advertencia cuando las operaciones de tratamiento previstas puedan infringir lo dispuesto en la normativa de protección de datos.
  En cuanto a la *«Advertencia»*, no debe considerarse un poder correctivo de tipo sancionador, toda vez que se limita - con anterioridad a quedar acreditada una determinada infracción - a notificar al responsable o encargado la posibilidad que de seguir en su conducta podría incurrir en infracción, así como recomendar el cese de un supuesto tratamiento que podría devenir en infracción. Debiendo entenderse no como una medida sancionadora sino «correctora», dirigida a corregir o subsanar el posible incumplimiento de la legislación de protección de datos por parte del responsable o encargado del tratamiento, y de cuya inobservancia se puede derivar incoación del correspondiente expediente sancionador, en los términos establecidos en el art. 65.3 de la LOPD. Se debe añadir que la norma no limita el número de «Advertencias» que se puedan notificar a un mismo responsable.
  Según la LOPDGDD, No procederá la iniciación del procedimiento sancionador, aun cuando se hubiere formulado reclamación, en los casos en que el encargado o responsable del tratamiento, previa advertencia formulada por una Autoridad de Control, haya adoptado las medidas correctivas encaminadas a poner fin al posible incumplimiento de la legislación de protección de datos, siempre que no se haya causado perjuicio al afectado y/o que el derecho del afectado quede plenamente garantizado mediante la aplicación de las medidas impuestas.
  Por último, y a efectos meramente didácticos, es plausible que la futura doctrina armonizada de las diferentes Autoridades de Control haga uso de la Advertencia sólo en aquellos casos en los que la posible infracción de la que trae causa pueda responder a infracciones de carácter meramente formal entre las dispuestas en el artículo 83.4 y 5 del RGPD.
- Sancionar a toda persona responsable o encargado del tratamiento con apercibimiento cuando las operaciones de tratamiento hayan infringido lo dispuesto en la normativa de protección de datos.
  El RGPD, prevé la posibilidad de que la sanción económica sea sustituida por un apercibimiento, para que el infractor adopte las medidas correctoras que se le indiquen.
  En todo caso, esta posibilidad es una medida excepcional.
  En este sentido, la AEPD tiene potestad discrecional para aplicarla en función de la naturaleza de los hechos.
  Cuando la AEPD apercibe en lugar de imponer una sanción económica, el responsable del fichero o el encargado del tratamiento deberán acreditar la adopción de las medidas correctoras indicadas por la AEPD en su resolución de apercibimiento. En caso de no acreditarse el cumplimiento de estas medidas, la AEPD ordenará la apertura de un procedimiento sancionador por dicho incumplimiento, pudiendo imponer una sanción por infracción muy grave.
  La AEPD ha aplicado el apercibimiento como alternativa a la sanción económica en numerosas ocasiones.

Por ejemplo:

- *Por el hecho de instalar un sistema de videovigilancia en las zonas comunes de la empresa sin informar a los afectados.*
- *Por el hecho de informar a los clientes de la creación de la página web de la empresa enviándoles un correo electrónico sin copia oculta (de manera que todos los destinatarios podían ver las direcciones de los demás).*

En cambio, se ha denegado el apercibimiento y se ha impuesto una multa en los casos de:

- *Abandono de documentos en la vía pública*
- *Envío de comunicaciones comerciales por e-mail o SMS sin el consentimiento previo y expreso de los destinatarios (salvo si éstos eran clientes de la empresa).*
- *Envío de mensajes electrónicos a destinatarios múltiples sin copia oculta (se trataba de datos especialmente protegidos).*
- *Difusión en una red social del parte de baja médica de una empleada.*
- *Publicidad en Internet de datos médicos por parte de una clínica (aunque se trató de un error puntual).*
- *Difusión en Internet por parte de la empresa del currículum de un trabajador.*

Sobre el apercibimiento, el considerando 148 del RGPD especifica lo siguiente:

> *«A fin de reforzar la aplicación de las normas del presente Reglamento, cualquier infracción de este debe ser castigada con sanciones, incluidas multas administrativas, con carácter adicional a medidas adecuadas impuestas por la autoridad de control en virtud del presente Reglamento, o en sustitución de estas. En caso de infracción leve, o si la multa que probablemente se impusiera constituyese una carga desproporcionada para una persona física, en lugar de sanción mediante multa puede imponerse un apercibimiento. Debe no obstante prestarse especial atención a la naturaleza, gravedad y duración de la infracción, a su carácter intencional, a las medidas tomadas para paliar los daños y perjuicios sufridos, al grado de responsabilidad o a cualquier infracción anterior pertinente, a la forma en que la autoridad de control haya tenido conocimiento de la infracción, al cumplimiento de medidas ordenadas contra el responsable o encargado, a la adhesión a códigos de conducta y a cualquier otra circunstancia agravante o atenuante. La imposición de sanciones, incluidas las multas administrativas, debe estar sujeta a garantías procesales suficientes conforme a los principios generales del Derecho de la Unión y de la Carta, entre ellas el derecho a la tutela judicial efectiva y a un proceso con todas las garantías».*

En la resolución de Apercibimiento se establecerán las medidas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción que se hubiese cometido. Al igual que en el caso de la Advertencia, el RGPD no limita el número de Apercibimientos a un responsable o encargado del tratamiento).

- Ordenar a la persona responsable o encargado del tratamiento que atiendan las solicitudes de ejercicio de los derechos del interesado en virtud del presente RGPD.

- Ordenar a la persona responsable o encargado del tratamiento que las operaciones de tratamiento se ajusten a las disposiciones de la normativa de protección de datos, cuando proceda, de una determinada manera y dentro de un plazo especificado.
- Ordenar a la persona responsable del tratamiento que comunique a la persona interesada las brechas de seguridad de los datos personales.
- Imponer una limitación temporal o definitiva del tratamiento, incluida su prohibición.
- Ordenar la rectificación o supresión de datos personales o la limitación de tratamiento con arreglo a los artículos 16, 17 y 18 y la notificación de dichas medidas a los destinatarios a quienes se hayan comunicado datos personales con arreglo a al artículo 17, apartado 2, y al artículo 19 del RPGD.
- Retirar una certificación u ordenar al organismo de certificación que retire una certificación emitida con arreglo a los artículos 42 y 43 del RGPD, u ordenar al organismo de certificación que no se emita una certificación si no se cumplen o dejan de cumplirse los requisitos para la certificación.
- Imponer una multa administrativa con arreglo al artículo 83 del RGPD, además o en lugar de las medidas mencionadas en el presente apartado, según las circunstancias de cada caso particular.
- Ordenar la suspensión de los flujos de datos hacia un destinatario situado en un tercer país o hacia una organización internacional.

II.2. Sujetos responsables

La LOPDGDD (artículo 70) establece un régimen sancionador sometido al establecido por el RGPD, aplicándose a los siguientes sujetos:

- Responsable de tratamiento: se trata de un concepto funcional, que designa a la persona que tiene la capacidad para decidir que se realice un tratamiento de datos para sus propios fines, capacidad derivada de una norma jurídica que le atribuye de forma expresa o de manera implícita, la competencia para decidir. El responsable del tratamiento decide «por qué» y «cómo» deberán tratarse los datos personales.
  La decisión sobre la realización de un tratamiento con una finalidad (determinación de los fines del tratamiento) lleva consigo la asunción del papel de responsable del tratamiento.
- Encargados de tratamiento: es la persona física o jurídica, autoridad pública, servicio u otro organismo que presta un servicio al responsable que conlleva el tratamiento de datos personales por cuenta de éste.
  Los tipos de encargado del tratamiento y las formas en que se regulará su relación pueden ser tan variados como los tipos de servicios que puedan suponer acceso a datos personales.
  Así podemos encontrar servicios cuyo objeto principal es el tratamiento de datos personales (por ejemplo, una empresa o entidad pública que ofrece un servicio de alojamiento de información en sus servidores) y otros que tratan datos personales sólo como consecuencia de la actividad que presta por cuenta del responsable del tratamiento (por ejemplo, el gestor de un servicio público municipal).

- Representantes de responsable o encargado de tratamiento no establecidos en UE (cuando sea de aplicación el artículo 3.2 del Reglamento, el responsable o el encargado del tratamiento designará por escrito un representante en la Unión).
- Entidades de certificación: aquellas que han sido acreditadas por la Entidad Nacional de Acreditación – ENAC-.
- Entidades supervisión de códigos de conducta: son aquellos organismos acreditados por la autoridad de control competente para supervisar un código de conducta, por tener el nivel adecuado de pericia en relación con el objeto del código, en virtud de lo señalado en el art. 40 del Reglamento.

El Delegado de Protección de Datos DPD, queda al margen de dicho régimen sancionador.

En el procedimiento sancionador cabe señalar que, si bien no hay distinción en función de la naturaleza pública o privada del infractor, sí existen diferencias en las sanciones que pueden imponerse, así en el supuesto de que el infractor tenga naturaleza privada, se puede resolver con una sanción económica o con un apercibimiento, y si el infractor tiene naturaleza pública se sanciona con apercibimiento. Tanto la multa como el apercibimiento pueden ir acompañados de medidas correctoras de las infracciones.

II.3. Infracciones

El Reglamento como norma jurídica vinculante establece en un único artículo (art. 83) prácticamente los principios básicos de la potestad sancionadora (legalidad, tipicidad, responsabilidad y proporcionalidad) así como las cuantías máximas de las correspondientes sanciones, si bien un tanto «sui generis» por cuanto no establece una cuadro de infracciones ni una categorización de las mismas, lo cual cabe inducir por la cuantía de las sanciones máximas que se establecen en los apartados 4, 5 y 6 de dicho artículo.

La LOPDGDD dando cumplimiento a lo señalado en el Reglamento, preceptúa como infracciones tanto aquellas conductas que contradigan el mismo: *«...infracciones del presente Reglamento indicadas en los apartados 4, 5 y 6...»,* así como las que resulten contrarias a la propia ley orgánica (art. 71).

En los artículos 72 al 74, ésta norma categoriza las distintas infracciones en muy graves, graves y leves.[8]

Observando el cuadro de infracciones diseñado, cabe destacar que no sólo hace una remisión genérica al RGPD para sancionar las conductas contrarias al mismo, sino que completa los elementos del tipo infractor y concreta aquellos artículos de éste cuya vulneración es objeto de sanción.

Por lo que concierne a los plazos de prescripción, en los citados artículos se señala que las infracciones muy graves prescribirán a los 3 años (art. 72.1), las

[8] Con respecto a las infracciones muy graves que se contemplan en el artículo 72 de la LOPDGDD y dadas las actuales circunstancias cabría hacer referencia a la prohibición establecida en el artículo 72.1.e) así la pandemia originada por el Covid-19, nos lleva a detenernos en una de las exenciones a la prohibición en el tratamiento de categorías especiales de datos, como es la recogida en el artículo 9.2.i) del RGPD:

graves a los 2 años (art 73.1) y las leves al año (art 74.1), de haberse cometido. Por lo tanto, el correspondiente procedimiento sancionador habrá de incoarse antes de que transcurran dichos plazos, de manera que una vez incoado este, la prescripción quedará interrumpida, reiniciándose el plazo de prescripción si el expediente sancionador estuviere paralizado durante más de seis meses por causas no imputables al presunto infractor (art. 75).

Cuando la Agencia Española de Protección de Datos ostente la condición de autoridad de control principal y deba seguirse el procedimiento previsto en el artículo 60 del RGPD interrumpirá la prescripción el conocimiento formal por el interesado del proyecto de acuerdo de inicio que sea sometido a las autoridades de control interesadas.

II.4. Sanciones

El Reglamento en su artículo 83, apartados 4, 5 y 6, establece unos límites máximos para las sanciones en función de la infracción cometida:

> *«4. Multa de 10 000 000 € como máximo o, tratándose de una empresa, de una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía; por infracciones de las disposiciones siguientes:*
>
> *a) las obligaciones del responsable y del encargado a tenor de los artículos 8, 11, 25 a 39, 42 y 43;*
>
> • Artículo 8 (consentimiento de los menores)
> • Artículo 11 (tratamientos que no requieren identificación).
> • Artículo 25 (protección de datos desde el diseño y por defecto).
> • Artículo 26 (corresponsables del tratamiento).
> • Artículo 27 (representantes de responsables o encargados no establecidos en la Unión).
> • Artículo 28 (encargado del tratamiento)
> • Artículo 29 (tratamiento bajo la autoridad del responsable o del encargado del tratamiento).
> • Artículo 30 (registro de actividades del tratamiento).
> • Artículo 31 (cooperación con la autoridad de control).
> • Artículo 32 (seguridad del tratamiento).
> • Artículos 33 (notificación de violaciones de seguridad)
> • Artículos 34 (comunicación de violaciones de seguridad)
> • Artículo 35 (evaluación relativa a la protección de datos)
> • Artículo 36 (consulta previa).
> • Artículo 37 (designación del delegado de protección de datos)
> • Artículo 38 (posición del delegado de protección de datos)
> • Artículo 39 (funciones del delegado de protección de datos)

«*el tratamiento es necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, sobre la base del Derecho de la Unión o de los Estados miembros que establezca medidas adecuadas y específicas para proteger los derechos y libertades del interesado, en particular el secreto profesional*».

b) las obligaciones de los organismos de certificación a tenor de los artículos 42 y 43;

c) las obligaciones de la autoridad de control a tenor del artículo 41, apartado 4.

5. Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 20 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

a) los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento a tenor de los artículos 5, 6, 7 y 9;

b) los derechos de los interesados a tenor de los artículos 12 a 22;

c) las transferencias de datos personales a un destinatario en un tercer país o una organización internacional a tenor de los artículos 44 a 49;

d) toda obligación en virtud del Derecho de los Estados miembros que se adopte con arreglo al capítulo IX;

- Artículo 85: Tratamiento y libertad de expresión y de información.
- Artículo 86: Tratamiento y acceso del público a documentos oficiales.
- Artículo 87: Tratamiento del número nacional de identificación.
- Artículo 88: Tratamiento en el ámbito laboral.
- Artículo 89: Garantías y excepciones aplicables al tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos.
- Artículo 90: Obligaciones de secreto.
- Artículo 91 Normas vigentes sobre protección de datos de las iglesias y asociaciones religiosas.

e) el incumplimiento de una resolución o de una limitación temporal o definitiva del tratamiento o la suspensión de los flujos de datos por parte de la autoridad de control con arreglo al artículo 58, apartado 2, o el no facilitar acceso en incumplimiento del artículo 58, apartado 1.

6. El incumplimiento de las resoluciones de la autoridad de control a tenor del artículo 58, apartado 2, se sancionará de acuerdo con el apartado 2 del presente artículo con multas administrativas de 20 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía.

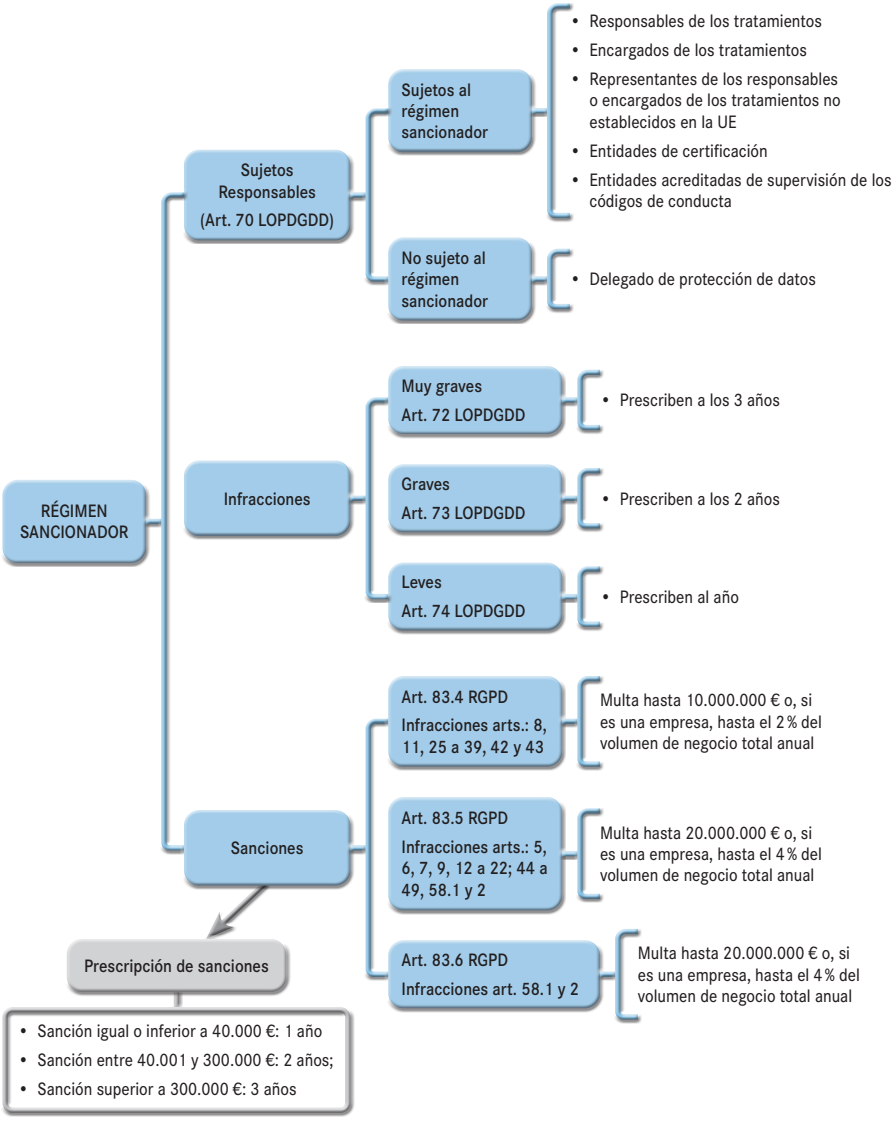
En correspondencia con la prescripción de sanciones (art. 78 LOPDGDD), en base al importe de la multa se establecen los siguientes plazos:

- Importe ≤ a los 40.000€ prescriben en el plazo de un año
- Importe comprendido entre 40.001 y 300.000 € a los dos años;
- Importe > a los 300.000 € a los tres años.

Cómputo: Este plazo de prescripción de las sanciones comenzará a contarse desde el día siguiente a aquel en que adquiera firmeza la resolución por la que se impone la sanción o haya transcurrido el plazo para recurrirla.

La prescripción se interrumpirá por la iniciación, con conocimiento del interesado, del procedimiento de ejecución, volviendo a transcurrir el plazo si el mismo está paralizado durante más de seis meses por causa no imputable al infractor.

Cuadro resumen de este proceso en la LOPDGDD:



II.6. El régimen sancionador para autoridades y organismos públicos

El Art.83.7 del Reglamento establece:

> *"Sin perjuicio de los poderes correctivos de las autoridades de control en virtud del artículo 58, apartado 2, cada Estado miembro podrá establecer normas sobre si se puede, y en qué medida, imponer multas administrativas a autoridades y organismos públicos establecidos en dicho Estado miembro".*

En cumplimiento de lo señalado en dicha disposición la LOPDGDD en su artículo 77 dispone:

> Régimen aplicable a determinadas categorías de responsables o encargados del tratamiento.
>
> *1. El régimen establecido en este artículo será de aplicación a los tratamientos de los que sean responsables o encargados:*
>
> *a) Los órganos constitucionales o con relevancia constitucional y las instituciones de las comunidades autónomas análogas a los mismos.*
>
> *b) Los órganos jurisdiccionales.*
>
> *c) La Administración General del Estado, las Administraciones de las comunidades autónomas y las entidades que integran la Administración Local.*
>
> *d) Los organismos públicos y entidades de Derecho público vinculadas o dependientes de las Administraciones Públicas.*
>
> *e) Las autoridades administrativas independientes.*
>
> *f) El Banco de España.*
>
> *g) Las corporaciones de Derecho público cuando las finalidades del tratamiento se relacionen con el ejercicio de potestades de derecho público.*
>
> *h) Las fundaciones del sector público.*
>
> *i) Las Universidades Públicas.*
>
> *j) Los consorcios.*
>
> *k) Los grupos parlamentarios de las Cortes Generales y las Asambleas Legislativas autonómicas, así como los grupos políticos de las Corporaciones Locales.*
>
> *2. Cuando los responsables o encargados enumerados en el apartado 1 cometiesen alguna de las infracciones a las que se refieren los artículos 72 a 74 de esta ley orgánica, la autoridad de protección de datos que resulte competente dictará resolución sancionando a las mismas con apercibimiento. La resolución establecerá asimismo las medidas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción que se hubiese cometido.*
>
> *La resolución se notificará al responsable o encargado del tratamiento, al órgano del que dependa jerárquicamente, en su caso, y a los afectados que tuvieran la condición de interesado, en su caso.*
>
> *3. Sin perjuicio de lo establecido en el apartado anterior, la autoridad de protección de datos propondrá también la iniciación de actuaciones disciplinarias cuando existan indicios suficientes para ello. En este caso, el procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario o sancionador que resulte de aplicación.*
>
> *Asimismo, cuando las infracciones sean imputables a autoridades y directivos, y se acredite la existencia de informes técnicos o recomendaciones para el tratamiento que no hubieran sido debidamente atendidos, en la resolución en la que se imponga la sanción se incluirá una amonestación con denominación del cargo responsable y se ordenará la publicación en el Boletín Oficial del Estado o autonómico que corresponda.*

4. Se deberán comunicar a la autoridad de protección de datos las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieren los apartados anteriores.

5. Se comunicarán al Defensor del Pueblo o, en su caso, a las instituciones análogas de las comunidades autónomas las actuaciones realizadas y las resoluciones dictadas al amparo de este artículo.

6. Cuando la autoridad competente sea la Agencia Española de Protección de Datos, esta publicará en su página web con la debida separación las resoluciones referidas a las entidades del apartado 1 de este artículo, con expresa indicación de la identidad del responsable o encargado del tratamiento que hubiera cometido la infracción.

Cuando la competencia corresponda a una autoridad autonómica de protección de datos se estará, en cuanto a la publicidad de estas resoluciones, a lo que disponga su normativa específica".

A pesar de que el Reglamento posibilita a que los Estados puedan imponer multas a los responsables o encargados del tratamiento pertenecientes a las administraciones públicas, se ha sustituido las sanciones económicas por la amonestación a través del apercibimiento, pero si bien pudiere parecer leve, el hecho de que la AEPD, publique en su página web la identidad del responsable o encargado del tratamiento que haya cometido la infracción, incide de manera bastante negativa en el crédito o prestigio que ha de tener dicho responsable o encargado. A su vez la autoridad de protección de datos no solo apercibirá al infractor, sino que cuando existan indicios suficientes para ello, propondrá contra el mismo la iniciación de actuaciones disciplinarias, en el marco del régimen disciplinario que le sea de aplicación, por lo que pudiere parecer a priori el apercibimiento como una sanción leve, puede conducir a otras que en el ámbito disciplinario tenga una respuesta de mayor gravedad, pudiendo derivar no sólo en efectos económicos, cuando por ejemplo se imponga una pérdida de haberes etc, sino la incidencia que pueda tener a efectos profesionales (suspensión de empleo, pérdida de destino, separación de servicio, etc).

En las infracciones cometidas por los órganos y organismos del Sector Público ha de tenerse en cuenta lo siguiente:

- Serán sancionadas con un apercibimiento con medidas correctoras y no tendrán sanción económica.
- La resolución sancionadora de la AEPD identificará el cargo responsable de la infracción, se notificará al infractor, a su superior jerárquico, al Defensor del Pueblo y se publicará en la página web de la AEPD[9] y en el diario oficial correspondiente.
- La resolución sancionadora podrá proponer al órgano u organismo la iniciación de actuaciones disciplinarias, cuya resolución deberá ser comunicada por el órgano u organismo del Sector Público a la AEPD.
- Las infracciones sean imputables a autoridades y directivos del Sector Público y se acredite la existencia de informes técnicos o recomendaciones que no hubieran sido atendidos por estos, la resolución sancionadora incluirá una amonestación con la identificación del cargo responsable y se publicará en el diario oficial correspondiente.

[9] https://www.aepd.es/es/informes-y-resoluciones/resoluciones

En resumen, podría argumentarse que, en el Derecho de la UE, el artículo 83 del RGPD faculta a las autoridades de control de los Estados miembros para imponer multas por infracciones del Reglamento. En el mismo artículo 83 se establecen los niveles de las multas y las circunstancias que las autoridades nacionales han de tener en cuenta para decidir si imponen una multa, así como los límites máximos totales de dicha multa. El régimen sancionador está, por tanto, armonizado para toda la UE.

El RGPD establece multas de distintos niveles. Las autoridades de control están facultadas para imponer multas administrativas por infracciones del Reglamento de hasta 20 000 000 EUR o, tratándose de una empresa, del 4 % de su volumen de negocio total anual global, optándose por la de mayor cuantía. Entre las infracciones que pueden dar lugar a multas de este nivel están las violaciones de los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento, las violaciones de los derechos de los interesados y las violaciones de las disposiciones del Reglamento que regulan la transferencia de datos personales a destinatarios de terceros países. Por otras infracciones, las autoridades de control pueden imponer multas de hasta 10 000 000 EUR o, tratándose de una empresa, del 2 % de su volumen de negocio total anual global, optándose por la de mayor cuantía.

A la hora de determinar el tipo y nivel de la multa impuesta, las autoridades de control deben tener en cuenta una serie de factores. Por ejemplo, deben tomar en la debida consideración la naturaleza, gravedad y duración de la infracción, las categorías[10] de datos personales afectadas y si existía intencionalidad o negligencia.

Cuando un responsable o encargado haya tomado medidas para paliar los daños y perjuicios sufridos por los interesados, esto también deberá tenerse en cuenta.; del mismo modo, el grado de cooperación con la autoridad de control tras la infracción y la forma en que la autoridad de control tuviera conocimiento de la misma (por ejemplo, si fue notificada por la entidad responsable del tratamiento o por un interesado cuyos derechos fueron vulnerados) son otros factores importantes que las autoridades de control deben tener en cuenta en su decisión .

Además de la capacidad de imponer multas administrativas, las autoridades de control tienen a su disposición una gran variedad de poderes correctivos adicionales, los denominados poderes «correctivos» de las autoridades de control están recogidos en el artículo 58 del RGPD, estos van desde órdenes, advertencias y apercibimientos a responsables y encargados hasta la imposición de prohibiciones temporales o definitivas de las actividades de tratamiento.

---

[10] Especial consideración merecen las categorías especiales de datos que se recogen en el artículo 9 del RGPD y en artículo 9 de la LOPDP, y por los cuales los responsables y encargados del tratamiento han de velar con mayor rigor [(art.28.2.c) de la LOPDP].

Un ejemplo del incumplimiento de las correspondientes medidas en aras de velar por dicha categoría especial de datos, lo tenemos en la Resolución R/03077/2017, de la AEPD, por que sanciona a CAJAMAR, Caja Rural, Sociedad Cooperativa de Crédito, por una infracción del artículo 7.3 de la LOPD, tipificada como muy grave en el artículo 44.4.b) de la LOPD, con una multa de 40.001€, al considerar que: *«... CAJAMAR ha realizado un tratamiento automatizado de datos de carácter personal de la afectada relacionado con informaciones concernientes a un posible trastorno de salud de la misma, resultando por esta razón de plena aplicabilidad los principios y garantías expuestos en la normativa de protección de datos de carácter personal respecto de los datos especialmente protegidos».*

II.7. Fases del procedimiento

II.7.1. Presentación de reclamaciones

El RGPD en su Considerando 141 señala:

> *«Todo interesado debe tener derecho a presentar una reclamación ante una autoridad de control única, en particular en el Estado miembro de su residencia habitual, y derecho a la tutela judicial efectiva de conformidad con el artículo 47 de la Carta si considera que se vulneran sus derechos con arreglo al presente Reglamento o en caso de que la autoridad de control no responda a una reclamación, rechace o desestime total o parcialmente una reclamación o no actúe cuando sea necesario para proteger los derechos del interesado...».*

Tales derechos los plasma en sus artículos 77.1, 78.2 y 79.1, estableciendo que todo interesado, sin perjuicio de cualquier otro recurso administrativo o acción judicial, tendrá derecho a presentar una reclamación ante una autoridad de control si considera que el tratamiento de datos personales que le conciernen infringe el Reglamento.

Tanto en el Derecho del Consejo de Europa (Convenio 108 modernizado, cuyo protocolo, conocido como «Protocolo 108+» fue ratificado por España el pasado 28/01/2021) como en el Derecho de la UE, las personas físicas tienen derecho a presentar solicitudes y reclamaciones a la autoridad de control competente si consideran que el tratamiento de sus datos personales no se está efectuando con arreglo a la ley.

El Convenio 108 modernizado reconoce el derecho de los interesados a contar con la ayuda de una autoridad de control en el ejercicio de sus derechos con arreglo al Convenio, sea cual sea su nacionalidad o residencia. Las peticiones de ayuda solo podrán denegarse en circunstancias excepcionales y los costes y tasas relacionados con la ayuda no deberán ser sufragados por los interesados.

En el ordenamiento jurídico de la UE existen disposiciones similares. El RGPD requiere que las autoridades de control adopten medidas para facilitar la presentación de reclamaciones, por ejemplo, mediante la creación de un formulario de presentación de reclamaciones por medios electrónicos.

El interesado puede presentar la reclamación ante la autoridad de control del Estado miembro en el que tenga su residencia habitual, lugar de trabajo o lugar de la supuesta infracción. Las reclamaciones deben ser investigadas y la autoridad de control debe informar al reclamante sobre el curso y el resultado de la reclamación.

Las posibles infracciones cometidas por instituciones u órganos de la UE pueden ponerse en conocimiento del Supervisor Europeo de Protección de Datos. Si el SEPD no responde en un plazo de seis meses, la reclamación se considerará desestimada. Contra las decisiones del SEPD se pueden interponer recursos ante el TJUE en el marco del Reglamento (CE) nº 45/2001, que obliga a las instituciones y los órganos de la UE a cumplir con la normativa de protección de datos.

Debe existir posibilidad de recurrir las decisiones de una autoridad de control nacional ante los órganos jurisdiccionales. Esto se aplica tanto a los interesados como a los responsables y encargados del tratamiento que hayan participado en el procedimiento ante una autoridad de control.

Ej.: En septiembre de 2017, la Agencia Española de Protección de Datos multó a Facebook por violar varias normas de protección de datos. La autoridad de control condenó a la red social por recoger, conservar y tratar datos personales —incluso datos personales de categorías especiales— con fines publicitarios y sin obtener el consentimiento de los interesados. La decisión fue el resultado de una investigación realizada por iniciativa propia de la autoridad de control.

Presentada la reclamación por un interesado o por un organismo, la autoridad de control debe tramitar las reclamaciones, e investigar, en la medida oportuna, el motivo de la reclamación e informar al reclamante sobre el curso y el resultado de la investigación en un plazo razonable.

La LOPDGDD recoge que las reclamaciones tramitadas por la AEPD se rigen por lo dispuesto en el RGPD, en la LOPDGDD, por las disposiciones reglamentarias dictadas en su desarrollo y, en cuanto no las contradigan, con carácter subsidiario, por las normas generales sobre los procedimientos administrativos.

Su Título VIII regula los procedimientos tramitados en la AEPD con motivo de la presentación de una reclamación por la falta de atención de las solicitudes de ejercicio de los derechos reconocidos en los artículos 15 a 22 del RGPD, y los procedimientos en los que se investigue la existencia de una posible infracción de lo dispuesto en el RGPD y en la LOPDGDD.

Este título también resulta de aplicación a los procedimientos que tramite la AEPD en el ejercicio de las competencias atribuidas por otras leyes, como las atribuidas por la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, y por la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.

Un aspecto novedoso que introduce la LOPDGDD consiste en la necesidad de realizar de forma previa una evaluación de la admisibilidad a trámite de la reclamación. Serán inadmitidas las reclamaciones que no versen sobre cuestiones de protección de datos, carezcan de fundamento, sean abusivas o no se aporten elementos que permitan investigar la existencia de una infracción.

También podrán ser inadmitidas las reclamaciones cuando el responsable o encargado del tratamiento, previa advertencia formulada por la AEPD, hubiera adoptado las medidas correctivas encaminadas a poner fin al posible incumplimiento de la legislación de protección de datos y concurra alguna de las siguientes circunstancias:

a) Que no se haya causado perjuicio al afectado en el caso de infracciones consideradas leves.
b) Que el derecho del afectado quede plenamente garantizado mediante la aplicación de las medidas.

En los demás casos, la LOPDGDD habilita a la AEPD para que, antes de resolver sobre la admisión a trámite de la reclamación, remita la misma al delegado de protección de datos (DPD) que hubiera, en su caso, designado el responsable o

encargado del tratamiento, si el afectado presentase la reclamación ante la AEPD sin haberla planteado antes ante el DPD (cuando el interesado se dirija previamente al DPD, éste tendrá un plazo máximo de 2 meses para adoptar la decisión), para que comunique al afectado su decisión y responda a la AEPD en el plazo de 1 mes. Transcurrido dicho plazo sin que se comunique a la agencia la decisión adoptada, ésta continuará con el procedimiento.

En el mismo sentido, cuando el responsable o encargado del tratamiento contra el que se dirija la reclamación esté adherido a un código de conducta que hubiera establecido procedimientos extrajudiciales o de mediación de los conflictos en materia de protección de datos, la AEPD podrá remitir al organismo establecido la reclamación para que le dé respuesta en el plazo de un mes, y tramitarla en el caso de que se rechazase.

Cuando no se hubiera designado un delegado de protección de datos ni el responsable o encargado estuviera adherido a mecanismos de resolución extrajudicial de conflictos, la AEPD podrá remitir la reclamación al responsable o encargado del tratamiento, en cuyo caso el responsable o encargado deberá dar respuesta a la reclamación en el plazo de un mes.

La Agencia, tras el análisis de las referidas respuestas, adoptará la decisión sobre la admisión o inadmisión a trámite de la reclamación. Las reclamaciones serán inadmitidas a trámite cuando de la respuesta facilitada por el DPD, el organismo de supervisión de la aplicación de los códigos de conducta, el responsable del tratamiento o el encargado se desprenda que se han corregido las circunstancias puestas de manifiesto en la reclamación y adoptado las medidas necesarias para evitar situaciones similares.

De conformidad con lo dispuesto en la LOPDGDD, también determinará con carácter previo a la iniciación de cualquier actuación, incluida la admisión a trámite de una reclamación o el comienzo de actuaciones previas de investigación, examinar su competencia y determinar el carácter nacional o transfronterizo, en cualquiera de sus modalidades, del procedimiento a seguir.

Si la AEPD no fuera la Autoridad de control principal remitirá la reclamación formulada a la Autoridad de control principal que se considere competente, a fin de que por la misma se le dé el curso oportuno, y archivará provisionalmente el procedimiento hasta que la autoridad de control principal adopte una decisión, en cuyo caso informará al reclamante de la decisión adoptada por la Autoridad de control principal.

La decisión sobre la admisión o inadmisión a trámite, así como la que determine, en su caso, la remisión de la reclamación a la autoridad de control principal que se estime competente deberá notificarse al reclamante en el plazo de tres meses. Si transcurrido este plazo no se produjera dicha notificación, se entenderá que prosigue la tramitación de la reclamación.

Después de la admisión a trámite, en el supuesto de reclamaciones que pudieran dar lugar a un procedimiento sancionador, se pueden realizar actuaciones previas de investigación encaminadas a determinar la concurrencia de motivos que justifiquen la apertura del procedimiento sancionador y no podrán extenderse más de 12 meses a contar desde el acuerdo de admisión a trámite de la reclamación.

Las actuaciones de investigación también pueden iniciarse por acuerdo que decida su iniciación cuando la AEPD actúe por propia iniciativa o como conse-

cuencia de la comunicación que le hubiera sido remitida por la autoridad de control de otro Estado miembro de la Unión Europea, en cuyo caso el plazo de 12 meses se computa a partir de la fecha del referido acuerdo de iniciación.

II.7.2. Iniciación del expediente

Una vez iniciado el procedimiento sancionador, como especialidad de este procedimiento, éste tendrá una duración máxima de 9 meses.

Sin embargo, cuando el procedimiento se refiera exclusivamente a la falta de atención de una solicitud de ejercicio de los derechos establecidos en los artículos 15 a 22 del RGPD, el procedimiento se iniciará por el acuerdo de admisión a trámite y su duración no podrá exceder del plazo de seis meses.

Ambos plazos son de caducidad, por lo que, decretado el archivo de actuaciones, si la infracción no ha prescrito, puede iniciarse nuevo expediente contra el presunto responsable de la misma.

Como se menciona previamente, las resoluciones que pongan fin a los procedimientos de reclamación serán objeto de publicación[11].

Establece el RGPD que toda persona física o jurídica tendrá derecho a la tutela judicial efectiva contra una decisión jurídicamente vinculante que le concierna de una autoridad de control. Las resoluciones de la AEPD agotan la vía administrativa y, por tanto, pueden ser objeto de recurso de reposición, ante la propia AEPD, y de recurso contencioso administrativo ante la jurisdicción de la Sala de lo Contencioso Administrativo de la Audiencia Nacional.

El Delegado de Protección de Datos del órgano u organismo del Sector Público debe recibir las reclamaciones que les dirijan los administrados, cuando opten por esta vía antes de plantear una reclamación ante la AEPD, y comunicará la decisión adoptada al administrado en el plazo máximo de dos meses.

Asimismo, el DPD deberá recibir las reclamaciones que la AEPD decida trasladarle con carácter previo al inicio de un expediente sancionador. El Delegado debe comunicar la decisión adoptada al administrado y a la Agencia en el plazo máximo de un mes. De esta forma, con carácter general, si el Delegado de Protección de Datos consigue que el responsable resuelva por cualquiera de estas dos vías la reclamación, y sin perjuicio de que el interesado posteriormente se dirija a la AEPD, no se iniciaría expediente de declaración de infracción a esa Administración Pública.

La Agencia tiene establecidos los cauces a seguir en función de las materias sobre las que versen las correspondientes reclamaciones (*publicidad y comunicación comercial, publicación de datos en internet, videovigilancia, etc*).

El procedimiento de denuncia de un tratamiento inadecuado de datos personales ante la AEPD sería a modo de ejemplo el siguiente:

- Antes de interponer una reclamación en el ejercicio de los derechos de acceso, rectificación, oposición, supresión («derecho al olvido»), limitación del tratamiento, portabilidad, el interesado se debe dirigir a la persona responsable del fichero por un medio que permita acreditarlo y ejercerlos.

[11] https://www.aepd.es/es/informes-y-resoluciones/resoluciones

  - 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
  - Las solicitudes deben responderse en el plazo de un mes, aunque, si se tiene en cuenta la complejidad y número de solicitudes, se puede prorrogar el plazo otros dos meses más.
  - El responsable está obligado a informarte sobre los medios para ejercitar estos derechos. Estos medios deben ser accesibles y no se puede denegar este derecho por el solo motivo de que optes por otro medio.
  - 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.
- Si el responsable no ha respondido en el plazo de un mes o si el ciudadano considera que la respuesta no ha sido adecuada, puede interponer una reclamación ante la Autoridad de Control.
- Si se tiene pruebas o indicios de un incumplimiento o infracción de la normativa de protección de datos que afecte al tratamiento de los datos personales, se puede presentar una reclamación ante la AEPD aportando dichos documentos. La tramitación es más ágil en los casos en que se aportan más pruebas o indicios junto con la denuncia, puesto que no se atenderá las reclamaciones sobre la presunta vulneración del tratamiento de tus datos personales si no se especifican los motivos concretos de tu solicitud o queja, o no existen indicios que permitan investigar.
- Puede presentar una denuncia cualquier persona que tenga conocimiento que se está vulnerando la normativa sobre protección de datos, aunque no sea la persona afectada por la presunta infracción.
- Existe la posibilidad de que, en vez de interponer una reclamación, se pueda acudir al sistema de mediación gestionado por Autocontrol, al que se han adherido las principales operadoras de telecomunicaciones del mercado: Movistar, Tuenti, O2, Orange, Jazztel, Amena, Simyo, Vodafone, Ono, Másmóvil, Yoigo, Lebara, Llamaya, Happy Móvil y Pepephone. Las reclamaciones a través de dicho sistema se limitan a determinados supuestos (9 en concreto), tales como: seguir recibiendo comunicaciones comerciales (llamadas publicitarias, emails promocionales, etc.), pese a haber ejercido tu derecho de oposición o haberse inscrito en la Lista Robinson de Adigital.
- La AEPD, pone a disposición de la ciudadanía y de los responsables distintos medios, así como guías y herramientas a través de los cuales se pue-

den presentar solicitudes de información, quejas o reclamaciones, y obtener información o asesoramiento que se precise[12], (ejemplo: el «Canal Prioritario», que ofrece una vía para denunciar la publicación ilegítima en Internet de contenidos sensibles, sexuales o violentos, incluso sin ser la persona afectada y donde se puede solicitar la eliminación urgente, en menos de 72 horas, de tales contenidos, especialmente si se trata de menores de edad o de víctimas de violencia por razón de género).

II.7.3. Intervención de las FCS en el procedimiento sancionador en materia de protección de datos

- Remisión de denuncias presentadas por los ciudadanos a la AEPD, en función del principio de colaboración interadministrativa [art. 31.k) de la LRJSP] además de la imposición establecida al efecto por el art. 14.1 de la LRJSP:

> *«El órgano administrativo que se estime incompetente para la resolución de un asunto remitirá directamente las actuaciones al órgano que considere competente, debiendo notificar esta circunstancia a los interesados».*

- Colaborar con la AEPD dentro de sus facultades inspectoras, a fin de acreditar y aportar aquellos elementos de prueba que sean necesarios para la determinación de la conducta infractora, en atención a lo señalado en el artículo 52.1 de la LOPDGDD:

> *«Las Administraciones Públicas, incluidas las tributarias y de la Seguridad Social, y los particulares estarán obligados a proporcionar a la Agencia Española de Protección de Datos, los datos, informes, antecedentes y justificantes necesarios para llevar a cabo su actividad de investigación».*

(Ej. Procedimiento Nº: PS/00156/2020 de la AEPD:

> *«HECHOS*
>
> *PRIMERO: A.A.A. (*en adelante, el reclamante) con fecha 3 de enero de 2020 interpuso reclamación ante la Agencia Española de Protección de Datos. La reclamación se dirige contra COMUNIDAD DE PROPIETARIOS ***DIRECCIÓN.1 con CIF H11257912 (en adelante, el reclamado).*
>
> *Los motivos en que basa la reclamación son se constata la presencia de una cámara orientada hacia la puerta de entrada del edificio sito en C/ ***DIRECCIÓN.1 (***LOCALIDAD.1), "teniendo conocimiento de que las imágenes obtenidas pudieran ser ilegales».*
>
> *Junto a la reclamación aporta prueba documental (Doc. nº 2) que acredita la presencia del dispositivo sin cartel informativo alguno en la entrada del inmueble.*
> *(...)*

[12] https://www.aepd.es/es

*CUARTO: Con fecha 14/10/20 se solicita colaboración a las Fuerzas y Cuerpos de Seguridad del Estado (***LOCALIDAD.1), para que constaten la presencia de la cámara y la legalidad del sistema.*

QUINTO: Con fecha 08/02/21 se vuelve a requerir colaboración a las Fuerzas y Cuerpos de Seguridad del Estado, para que constaten la presencia de la cámara y la legalidad del sistema, realizando las indagaciones oportunas.

*SEXTO: En fecha 01/03/21 se recibe contestación Comisaría Provincial (***LOCALIDAD.1) trasladando Oficio en el cual se informa de lo siguiente: «En virtud de las funciones que tiene atribuidas esta unidad territorial de seguridad Privada referidas a las actuaciones de control e inspección (arts 53 y 54 de la Ley 5 / 14 de 4 de abril de Seguridad Privada) los agentes actuantes proceden a girar visita.*

Constatando efectivamente la existencia de una cámara de video-vigilancia ubicada en el lugar descrito enfocando a la vía pública portal de acceso al edificio. Verificando asimismo la ausencia del cartel informativo de la A.E.P.D. que indica el responsable del tratamiento, siendo todo ello consignado en el acta de inspección levantada al efecto».

A la vista de todo lo actuado, por parte de la Agencia Española de Protección de Datos
en el presente procedimiento se consideran hechos probados los siguientes,

(...)

Cuarto. Consta acreditada la presencia de dispositivo de grabación de imágenes orientado hacia zona de acera pública, estando mal orientada la cámara de video-vigilancia.

La cámara según constata la fuerza actuante está operativa, procediendo al «tratamiento de datos personales»).

II.7.4. Criterios de imposición de las multas administrativas

El RGPD en su artículo 83 apartados 1 al 3 establece:

- Las multas administrativas serán: efectivas, proporcionadas y disuasorias.
- Se impondrán en función de las circunstancias de cada caso individual, a título adicional o sustitutivo de las medidas correctivas impuestas por las autoridades de control relacionadas en el artículo 58, apartado 2, letras a) a h) y j).
- El incumplimiento intencionado o negligente de un responsable o encargado del tratamiento de diversas disposiciones del presente Reglamento, se sancionara con una multa no superior a la cuantía prevista para las infracciones más graves.

La imposición y graduación de las sanciones se rigen por los principios de responsabilidad y proporcionalidad, y en este sentido el Reglamento determina

que, para la imposición de una multa administrativa y su cuantía, se han tener en cuenta los siguientes criterios de graduación (art. 83.2):

a) la naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance o propósito de la operación de tratamiento de que se trate, así como el número de interesados afectados y el nivel de los daños y perjuicios que hayan sufrido;
b) la intencionalidad o negligencia en la infracción;
c) cualquier medida tomada por el responsable o encargado del tratamiento para paliar los daños y perjuicios sufridos por los interesados;
d) el grado de responsabilidad del responsable o del encargado del tratamiento, habida cuenta de las medidas técnicas u organizativas que hayan aplicado en virtud de los artículos 25 y 32; e) toda infracción anterior cometida por el responsable o el encargado del tratamiento;
f) el grado de cooperación con la autoridad de control con el fin de poner remedio a la infracción y mitigar los posibles efectos adversos de la infracción;
g) las categorías de los datos de carácter personal afectados por la infracción;
h) la forma en que la autoridad de control tuvo conocimiento de la infracción, en particular si el responsable o el encargado notificó la infracción y, en tal caso, en qué medida;
i) cuando las medidas indicadas en el artículo 58, apartado 2, hayan sido ordenadas previamente contra el responsable o el encargado de que se trate en relación con el mismo asunto, el cumplimiento de dichas medidas;
j) la adhesión a códigos de conducta en virtud del artículo 40 o a mecanismos de certificación aprobados con arreglo al artículo 42, y
k) cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso, como los beneficios financieros obtenidos o las pérdidas evitadas, directa o indirectamente, a través de la infracción.

Este último apartado ha posibilitado que se añadan nuevos criterios de graduación por parte de la LOPDGDD (art. 76.2):

a) El carácter continuado de la infracción.
b) La vinculación de la actividad del infractor con la realización de tratamientos de datos personales.
c) Los beneficios obtenidos como consecuencia de la comisión de la infracción.
d) La posibilidad de que la conducta del afectado hubiera podido inducir a la comisión de la infracción.
e) La existencia de un proceso de fusión por absorción posterior a la comisión de la infracción, que no puede imputarse a la entidad absorbente.
f) La afectación a los derechos de los menores.
g) Disponer, cuando no fuere obligatorio, de un delegado de protección de datos.
h) El sometimiento por parte del responsable o encargado, con carácter voluntario, a mecanismos de resolución alternativa de conflictos, en aquellos supuestos en los que existan controversias entre aquellos y cualquier interesado.

Las reclamaciones pueden plantearse directamente ante la Agencia, aunque también pueden llegar a través de alguna Autoridad de Control de los Estados miembros del Espacio Económico Europeo (EEE). Estas últimas tienen un carácter transfronterizo y se admiten a través del mecanismo de ventanilla única, establecido en el artículo 60 del RGPD.

Bien como consecuencia de las reclamaciones, bien por propia iniciativa, la persona titular de la Dirección de la Agencia puede ordenar la apertura de actuaciones de investigación para alcanzar un mejor conocimiento y determinación de las conductas o hechos que puedan infringir la normativa de protección de datos.

La Subdirección General de Inspección de Datos (SGID) es el órgano de la AEPD, dependiente de su Directora, que en caso de posible vulneración de la normativa o de no atención al ejercicio de derechos, analiza los indicios, realiza las actuaciones de tutela o de investigación oportunas y, cuando procede, instruye los procedimientos sancionadores para proponer a la Directora la adopción de la resolución que corresponda.

Asimismo, a ello hay que sumar la realización de planes sectoriales y auditorías preventivas, cuyo objetivo es dictar directrices que sirvan de guía en el cumplimiento de lo establecido reglamentariamente.

Dentro de los casos en los que se actúa por iniciativa propia hay que destacar las actuaciones de investigación que se realizan, cuando procede, a raíz de las notificaciones de brechas de seguridad en materia de protección de datos personales. Las notificaciones se efectúan de acuerdo con el artículo 33 del RGPD.

Estas brechas se reciben en primera instancia en la División de Innovación Tecnológica (DIT) de la AEPD y, tras un primer análisis, en los casos en los que resulta pertinente, se propone a la Directora que sean trasladadas a la Subdirección General de Inspección de Datos, donde se valora el inicio de una posible investigación. Dada la importancia que tienen, se analizan de manera independiente bajo el epígrafe de notificaciones de brechas de seguridad. Se contabilizan únicamente aquellas en las que la DIT determina que procede su evaluación y posible investigación por parte de la Subdirección General de Inspección de Datos.

Ejemplo:

Una empresa vende material para el hogar por internet. A través de su sitio web, los consumidores podían comprar electrodomésticos, mesas, sillas y otros artículos para el hogar introduciendo su información bancaria. El sitio web sufrió un ciberataque que puso la información personal a disposición del atacante. En este caso, la ausencia de medidas técnicas adecuadas por parte de la empresa parece haber sido la causa de la pérdida de los datos.

En este ejemplo, se tendrán en cuenta varios factores por parte de la autoridad de control antes de decidir qué instrumento correctivo debe utilizarse. Factores como los siguientes: la gravedad de la deficiencia en el sistema informático; el tiempo que estuvo expuesta a este riesgo la infraestructura informática; las pruebas realizadas en el pasado para evitar este tipo de ataque; el número de clientes de los que se robaron o divulgaron los datos; el tipo de datos personales que se vieron afectados (¿había datos sensibles?). La autoridad de control tendrá en cuenta todas estas consideraciones.

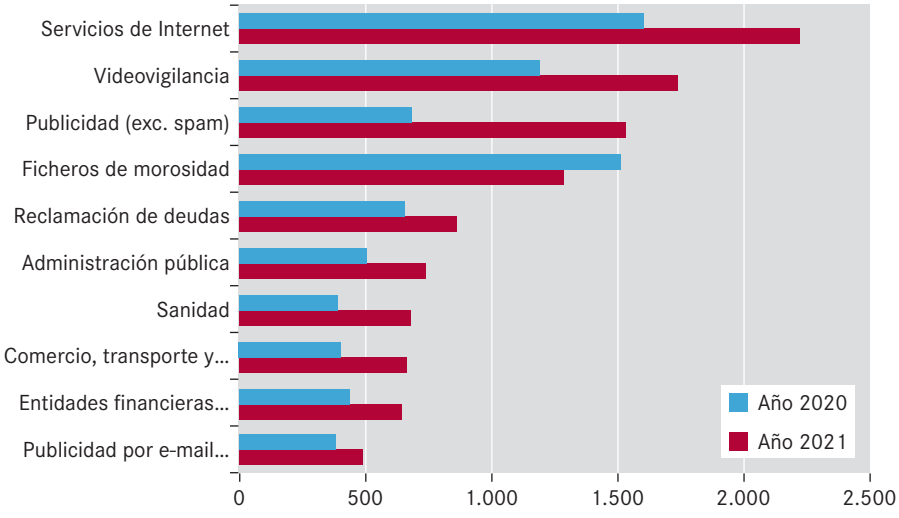
La LOPDGDD regula en su Título VIII (arts. 63 a 69) el procedimiento establecido en caso de posible vulneración de la normativa de protección de datos.

II.8. Estadísticas[13]

II.8.1. Reclamaciones

En el año 2020 se formularon un total de 10324, y en el año 2021 se elevó la cifra a 13905 lo que supone un incremento del 35% con respecto al año anterior, siendo las más frecuentes las comprendidas dentro de los 10 sectores de actividad que se muestran en el gráfico:

Reclamaciones más frecuentes ante la AEPD				
Sectores de actividad	**Año 2020**	**Año 2021**	**Variación**	**Diferencia %**
Servicios de Internet	1.602	2.220	618	28
Videovigilancia	1.189	1.736	547	32
Publicidad (excepto spam)	681	1.528	847	55
Ficheros de morosidad	1.510	1.284	-226	-18
Reclamación de deudas	656	859	203	24
Administración pública	503	740	237	32
Sanidad	388	680	292	43
Comercio, transporte y hostelería	405	663	258	39
Entidades financieras/acreedoras	437	643	206	32
Publicidad por e-mail o teléfono móvil	380	487	107	22
TOTAL TOP 10	7.727	10.840	**3.113**	**29**



[13] Datos obtenidos de la Memoria de la AEPD 2021.

Del total de reclamaciones presentadas en 2020 y en 2021, en torno al 60% fueron inadmitidas, pasando el resto a la apertura de actuaciones de investigación o de procedimiento.

Los procedimientos sancionadores incoados en 2021 fueron 585, de los cuales 264 se sancionaron con multa, 222 con apercibimiento y en 99 se dictó archivo de actuaciones.

En relación a los sectores más relevantes, como se puede observar con los datos del gráfico, a nivel general el número de reclamaciones aumentó en 2021 con respecto al 2020 en un 29% en los principales sectores que son objeto de las mismas, siendo los incrementos más acusados las relacionadas con la promoción publicitaria, la mayoría referidas a la recepción de llamadas telefónicas no deseadas, el ejemplo más representativo de ello es expediente sancionador incoado a Vodafone, iniciado a consecuencia de las más de 190 reclamaciones formuladas contra dicho operador de telefonía, por la práctica de acciones de mercadotecnia en nombre de dicha entidad a través de llamadas telefónicas y comunicaciones electrónicas (SMS y correo electrónico), resolviéndose el expediente en 2021, imponiéndole diversas multas por importe total de 8.150.000€.

En el año 2020, se han analizado 165 reclamaciones relacionadas con la captación y/o difusión de la imagen de miembros de las fuerzas y cuerpos de seguridad, en redes sociales y aplicaciones de mensajería, realizadas por particulares, la mayoría en el marco de operaciones policiales relacionadas con la verificación del efectivo cumplimiento de las restricciones gubernativas adoptadas durante el estado de alarma. Prácticamente todas estas reclamaciones han sido archivadas al no observarse vulneración de la normativa de protección de datos en los tratamientos afectados.

Debido a la situación de crisis sanitaria por el Covid-19, en el año 2020 fueron numerosas las reclamaciones sobre presentadas por particulares contra vecinos, que se dieron en denominar «policías de balcón», por la difusión en redes sociales de fotografías y vídeos con el objetivo de dar publicidad a supuestos incumplimientos de las mencionadas restricciones, generalmente en la vía pública; también reclamaciones referidas a incumplimientos legales en el tratamiento de datos sanitarios asociados a la pandemia, como por ejemplo un sitio web que, con garantías no suficientemente acreditadas, ofrecía contacto con profesionales médicos para la asistencia sanitaria online; o reclamaciones relacionadas con la toma de temperatura por personal que habitualmente realiza labores de vigilancia en la entrada, en el entorno laboral, en establecimientos comerciales y en lugares de culto religioso; asimismo han sido significativas las reclamaciones referidas a la vulneración del principio de confidencialidad asociado al dato de contagio por el coronavirus en distintos ámbitos, particularmente en el entorno laboral y en redes sociales y medios de comunicación.

En este contexto fueron especialmente numerosas las reclamaciones relacionadas con la situación excepcional que, por segundo año consecutivo, atravesamos con motivo de la citada pandemia, así deben destacarse las relacionadas con el tratamiento de datos asociados al cumplimiento de las medidas restrictivas establecidas por las autoridades sanitarias, vinculadas con la exhibición de datos de salud sobre las circunstancias que, en ciertos casos, eximen del uso de mascarilla o con la utilización del certificado COVID digital de la UE, por citar algunos ejemplos:

- Actuaciones previas de investigación sobre las medidas para hacer frente a la crisis sanitaria ocasionada por la COVID-19, aprobadas por la Comunidad de Madrid entre las que se hallaba la obligatoriedad para los salones de banquetes, discotecas y establecimientos de ocio nocturno de llevar un registro con datos de contacto de clientes para facilitar su localización en caso de confirmarse un caso positivo en alguno de estos establecimientos. Tras haberse ratificado dichas medidas por Auto del Juzgado de lo Contencioso Administrativo nº 8 de Madrid, por la AEPD se procede al archivo de las actuaciones.
- Actuaciones previas de investigación en relación con la instalación de cámaras fototérmicas a la entrada de los establecimientos de El Corte Inglés, para la toma de temperatura de trabajadores y clientes. Por lo que concierne a la toma de temperatura a los trabajadores, se trata de una obligación legal conforme a la Ley de Prevención de Riesgos Laborales, que no se realiza de manera aislada, sino en conjunto con otras medidas para la lucha contra la COVID19, previstas en un "Plan de contingencia para la reapertura de tiendas". Respecto a la toma de temperatura a los clientes, no queda acreditado que se hayan tratado datos personales de personas identificables, por lo que no resulta de aplicación el RGPD, por lo que la AEPD finaliza el expediente con el archivo de las actuaciones.
- Actuaciones previas de investigación a raíz de las noticias aparecidas en diversos medios de comunicación sobre la elaboración de un informe por parte el Ministerio del Interior, dirigido a la identificación, estudio y seguimiento, en relación con la situación creada por el COVID-19 de campañas de desinformación, así como publicaciones desmintiendo bulos y fake news susceptibles de generación de estrés social y desafección a instituciones del Gobierno, siendo archivadas las actuaciones, al no quedar acreditada la realización de tratamientos de datos de carácter personal.

En relación con las reclamaciones presentadas a través del Canal Prioritario, de las 377 peticiones presentadas, 31 de ellas se tramitaron como urgentes para la retirada de contenidos, después de su examen y teniendo en cuenta la naturaleza especialmente sensible de los datos personales divulgados y la afectación grave a la intimidad, se realizaron 25 intervenciones de urgencia procediéndose de inmediato a la retirada de los contenidos sensibles.

En relación con las brechas de seguridad de datos personales, se ha detectado un aumento de ataques por *«ransomware»* relacionados con la pandemia. Se trata de un software malicioso que se usa para extorsionar, cifrando la información almacenada en dispositivo –móvil u ordenador- solicitando el pago de una cantidad para liberar la información bloqueada.

Los datos interanuales muestran un ligero descenso en el número de notificaciones de brechas de seguridad a la AEPD durante 2021, siendo 76 frente a 81 del año 2020.

II.8.2. Sanciones

Tomando como referencia el último lustro (entre 2016 y 2021) la AEPD ha incoado 3488 expedientes sancionadores, dentro de los cuales destacamos los siguientes sectores:

- Contratación fraudulenta (522), videovigilancia (490), servicios de internet (288), publicidad a través de e-mail o teléfono móvil (284), telecomunicaciones (265), publicidad -excepto spam- (228), morosidad (192), morosidad en entidades financieras (116), entidades financieras (78), administración pública (65), comercios, transporte y hostelería (56), suministros de gas, electricidad y agua (49), sanidad (48), y en lo que respecta a las Fuerzas y Cuerpos de Seguridad se incoaron un total de 4 expedientes sancionadores en dicho periodo.
- Con respecto a las resoluciones sancionadoras dictadas en el mencionado marco temporal, se dictaron 1429 que correspondieron a procedimientos de apercibimiento y 295 a expedientes de infracción, de entre los cuales 5 correspondieron a Fuerzas y Cuerpos de Seguridad por infracciones a la anterior LOPD 15/1999 de 13 de diciembre, tipificadas en los artículos 4.1 (Calidad de los datos), 6.1 (consentimiento del afectado), 9 (Seguridad de los datos) y 10 (Deber de secreto).

En cuanto a las sanciones impuestas, se pueden mostrar los siguientes datos: En 2020 se impusieron 167 multas por un importe total de 8.018.800€, y en 2021 la cifra se incrementó a 258 multas por una cuantía que asciende a los 35.074.800€.

En número de multas, la AEPD supera al resto de autoridades de control europeas, sin que ello se corresponda con un mayor volumen en el importe de las sanciones con respecto al resto de países de nuestro entorno como a continuación veremos.

Sectores con sanciones de mayor cuantía			
Areas de actividad	**2020**	**2021**	**Δ interanual**
Publicidad (excepto spam)	17.700	8.659.200	48.922%
Telecomunicaciones	1.009.000	6.500.000	644%
Entidades financieras	5.045.000	6.243.000	124%
Ficheros de Morosidad	387.000	4.209.000	1.088%
Contratación fraudulenta	559.000	3.674.000	657%
Asuntos laborales	40.600	2.625.900	6.468%
Otros	960.500	3.163.700	329%
TOTAL	**8.018.800**	**35.074.800**	**437%**

Algunas de las sanciones más altas impuestas en nuestro país serían las siguientes:

- Google LLC,18 de mayo de 2022, por dos infracciones muy graves de la normativa de protección de datos, sancionado a dicha compañía con 10 millones de euros por ceder datos a terceros sin legitimación para ello y obstaculizar el derecho de supresión de los ciudadanos (artículos 6 y 17 del Reglamento General de Protección de Datos).
- Mercadona, 27 de julio de 2021, multa de 3,15 millones de euros (reducida a 2.520.000€ por pago voluntario), por diversas infracciones del RGPD

relacionadas con el sistema de reconocimiento facial implementado por Mercadona en varias de sus tiendas para evitar la entrada de personas que habían cometido un delito contra sus empleados o bienes, y que habían sido condenados en sentencia firme con una orden de alejamiento sobre las instalaciones de Mercadona.

- EDP Energía 1.500.000€ y EPD Comercializadora 1.500.000€, sanciones impuestas el pasado año contra dichas empresas, por el tratamiento de datos personales sin consentimiento del interesado. Estos tratamientos se producen en el marco de la contratación de servicios de electricidad o gas efectuadas supuestamente por un representante del cliente, sin que dicha entidad pueda acreditar la existencia de tal representación.
- Vodafone España el 11 de marzo de 2021, con 8,15 millones de euros (dividido en cuatro sanciones) fundamentalmente por la realización de acciones de mercadotecnia y de prospección comercial a través de llamadas telefónicas y mediante el envío de comunicaciones comerciales electrónicas, tanto de correos como de mensajes SMS; comunicaciones que no han sido solicitadas o expresamente autorizadas por las personas que las han recibido, que no han podido ejercer el derecho a oponerse o se han dirigido a personas que habían pedido su inclusión en la «lista Robinson» y no se adecuaban tampoco a los procedimientos y garantías establecidas para realizar esas acciones de mercadotecnia.
- CaixaBank en enero de 2021 y asciende a 6 millones de euros, al considerar que la entidad había infringido tres artículos del Reglamento al forzar la recogida de datos personales de sus clientes sin una base legal válida y no informarles de manera adecuada del tratamiento que iba a realizar sobre esa información.
- Un mes antes, en diciembre de 2020, la AEPD multó al BBVA con 5 millones de euros por el mismo motivo.

Tales sanciones se encuentran entre las más cuantiosas desde la entrada en vigor del Reglamento, si bien, para una mejor concreción de la situación es necesario aludir a que la Agencia, cumpliendo con la previsión legal contenida en el artículo 76.4 de la LOPDGDD, el 22 de febrero de 2022, publicó en el Boletín Oficial del Estado[14] la Resolución de 11 de febrero de 2022, por la que se publicaban las sanciones superiores a un millón de euros impuestas a personas jurídicas en el año 2021 y cuyo contenido material reproducimos a continuación:

Nombre del infractor	Infracción cometida	Importe sanción (euros)
Banco Bilbao Vizcaya Argentaria, S. A.	Artículo 13 del RGPD	5.000.000
	Artículo 14 del RGPD	
	Artículo 6 del RGPD	

[14] https://www.boe.es/boe/dias/2022/02/22/pdfs/BOE-A-2022-2846.pdf

Nombre del infractor	Infracción cometida	Importe sanción (euros)
Vodafone España, S. A. U.	Artículo 48.1.b) del LGT	8.150.000
	Artículo 21.1 de la LSSI	
	Artículo 28 del RGPD	
	Artículo 44 del RGPD	
EDP Energía, S. A. U.	Artículo 13 del RGPD	1.500.000
	Artículo 25 del RGPD	
EDP Comercializadora, S. A.	Artículo 25 del RGPD	1.500.000
	Artículo 13 del RGPD	
Mercadona, S. A.	Artículo 12 del RGPD	2.520.000
	Artículo 13 del RGPD	
	Artículo 25 del RGPD	
	Artículo 35 del RGPD	
	Artículo 5.1.c) del RGPD	
	Artículo 6 del RGPD	
	Artículo 9 del RGPD	

En relación con los sectores más sancionados, se recoge:

- El sector bancario: 11 millones de euros, siendo sin embargo el que menos multas acumula (un total de 7).
- Empresas telefónicas: 10.171.000€, con 50 multas.
- Le siguen compañías dedicadas al suministro de gas, electricidad y agua: 344000€ y 6 multas.
- Empresas que prestan servicios en internet: 203.400€, y 17 multas.
- Videovigilancia: 126.640€, y 35 multas.
- Comercio, transporte y hostelería: 86.700, y 15 multas.
- Sanidad: 48.000€, con una multa.
- Asuntos laborales: 40.600€ y 8 multas.
- Asociaciones, federaciones y clubes: 16.000€, con 3 multas
- Comunidades de propietarios: 10.000€ y una multa.

Los sectores con mayor volumen en el manejo de datos personales tales como el financiero, o el de las telecomunicaciones, son los que en proporción a esa gran cantidad de datos personales que manejan, lideran el ranking de las sanciones, lo conlleva la necesidad de extremar al máximo las medidas de seguridad en tales ámbitos.

Las infracciones más comunes se pueden agrupar en las causas siguientes:

- La primera causa de incumplimiento es la establecida por el artículo 6 del RGPD[15], al incumplir algunas de las condiciones que se establecen en dicho artículo para la licitud del tratamiento, siendo la principal que el responsable del tratamiento cuente con el consentimiento del interesado a la hora de recoger y utilizar su información personal.
- La segunda causa de incumplimiento más común es no facilitar información suficiente a los usuarios sobre el uso que se va a hacer de los datos personales recogidos, señalada en el artículo 13 del RGPD. Esta obligación consiste en informar al interesado sobre la identidad del responsable del tratamiento, la base jurídica sobre la que se sustenta la recogida de datos, el fin para el que se recopilan y si estos van a ser compartidos con terceros.
- La tercera causa más común es la falta de integridad y confidencialidad en el tratamiento, art. 5.1.f) del RGPD.
- Siguiendo la falta de licitud, lealtad y transparencia en el tratamiento, art. 5.1.a) RGPD
- Ocupando el quinto lugar la falta de exactitud en el tratamiento, art. 5.1.d) RGPD

Las empresas por la incidencia que ello se puede derivar para su prestigio, tratan de evitar en la mayor medida posible las brechas de seguridad, no siendo tan esmeradas en otros aspectos, no obstante tras el tiempo de adaptación otorgado por la AEPD, a lo que se suma la cuantía de las sanciones, las entidades poco a poco están concienciándose en su obligación de garantizar la privacidad de sus clientes; asimismo ello les refuerza su imagen institucional al considerarlo como un valor añadido frente a la competencia, al transmitir confianza y credibilidad a los clientes, de hecho en los últimos tiempos los departamentos de protección de datos y la figura del Delegado de Protección de datos al frente de los mismos se han convertido en una de las áreas fundamentales de las distintas entidades.

En 2021 ha sido notable el incremento del importe las multas impuestas por las autoridades europeas de protección de datos por infracciones al Reglamento General de Protección de Datos (RGPD), superando los 1.100 millones de euros, mientras que en 2020 la cifra ascendía a poco más de 171 millones de euros, 72 millones de euros en 2019 y 436.000 euros en 2018.

Respecto al sector de actividad con más sanciones, se puede observar que a nivel europeo encabezan la lista los medios de comunicación, las telecomunicaciones y la radiodifusión, mientras que en España el sector financiero, junto al de

[15] Un ejemplo reciente lo tenemos en la sentencia nº 4999/2021, de 5 de noviembre, de la Sala de lo Contencioso-Administrativo de la Audiencia Nacional, que desestima el recurso contencioso administrativo interpuesto por AVON COSMETIC SAU, frente a la resolución de la AEPD de 26 de julio de 2019, por la que se impone a dicha entidad una sanción por importe de 60.000, por una infracción del Artículo 6 del RGPD, tipificada en el Artículo 83.5 del RGPD, concluyendo que: *«... la entidad actora inició una relación comercial con una tercera persona sin control ni supervisión suficiente en cuanto no fue capaz de detectar que realmente, la persona que estaba manifestando su voluntad de contratar, no era quien decía ser. Tal y como deriva del referido RGPD, AVON, en cuanto responsable del tratamiento, y a pesar de sus extensas argumentaciones de la demanda, no ha sido ser capaz de demostrar que la denunciante había dado su consentimiento a la operación de tratamiento de sus datos personales».*

telecomunicaciones y al de energía, han sido los que mayores sanciones han recibido. Veamos los ejemplos más representativos de los países de nuestro entorno:

- Luxemburgo: La Comisión Nacional de Protección de Datos de Luxemburgo (CNPD) ha sancionado con 746 millones de euros a Amazon Europe Core, al considerar que el tratamiento de datos personales por parte de la multinacional no cumplía con la normativa sobre protección de datos de la Unión Europea.
- Irlanda: La Comisión para la Protección de Datos (DPC), ha impuesto una multa de 225 millones de euros a la compañía de mensajería móvil WhatsApp, por incumplir el Reglamento General de Protección de Datos de la UE, al no haber informado a sus usuarios de cómo estaba compartiendo su información con Facebook, compañía propietaria de aquella.
- Francia. la Autoridad de Control de Francia (CNIL) registro únicamente ocho multas, sancionando a Google con 50 millones de euros, por incumplimientos relacionados con el uso e instalación de cookies, la falta de obtención de un consentimiento previo a su instalación y deficiencias a la hora de suministrar la información al usuario; y a Amazon con 35 millones por el mismo motivo; el importe de las sanciones se determinó teniendo en cuenta, además de la naturaleza de los incumplimientos, el volumen de tráfico de usuarios que se produce en sus webs y los beneficios (ingresos publicitarios en el caso de Google e incremento de la visibilidad de sus productos en otras webs en el caso de Amazon) que indirectamente habrían obtenido a través del uso e instalación de las cookies en los dispositivos de los usuarios. Carrefour fue sancionado con 3 millones de euros por diversos incumplimientos del Reglamento General de Protección de Datos (RGPD)y del artículo 82 de la ley de protección de datos francesa que regula las cookies.
- Alemania: la Autoridad de Control alemana impuso tres multas en 2020, sancionando con 35,3 millones de euros, a H&M por recopilar información de sus trabajadores en bases de datos de forma ilícita, en concreto por vigilar a cientos de sus trabajadores en el centro de coordinación en Núremberg.
- Italia. la Autoridad de Control de Italia impuso una sanción de 27,8 millones de euros y otra de 16,7 a TIM y Wind Tre SPA, respectivamente, por el envío de comunicaciones comerciales sin consentimiento de los interesados, realizando miles de llamadas promocionales sin el consentimiento de los destinatarios, o pese al registro de estos en una lista Robinson, o incluso tras el ejercicio de estos de su derecho de oposición. Vodafone fue multada con 12,2 millones por «telemarketing masivo» sin consentimiento de los usuarios. Se utilizaron números ficticios y números no registrados en el Registro de Operadores de Comunicaciones para realizar dichos contactos telefónicos. Del mismo modo, se habrían utilizado listas de contacto adquiridas a través de proveedores externos, es decir, a través de socios comerciales de Vodafone donde dicha operadora se habrían obtenido los números de terceros sin su consentimiento. Y en el mes de marzo de 2020, esta autoridad ha sancionado con 20 millones de euros a la empresa «*Clearview* A.I» por haber introducido un sistema de «vigilancia biométrica» de las personas residentes en Italia.

- Reino Unido. La autoridad de protección de datos registró únicamente tres multas, pero imponiendo a British Airways 20 millones de libras (22 millones de euros), seguida de la cadena de hoteles Marriott 18,9 millones y, por último, Ticketmaster 1,2 millones, debido todas ellas a brechas de seguridad y filtración externa de datos.

Este incremento de las sanciones deja patente la vulnerabilidad que sufren las personas en materia de protección de datos personales, poniendo en evidencia los incumplimientos de la ley, cada vez más habituales, por parte de las empresas. Esto es debido, a que la información se ha convertido en un activo estratégico de primer orden, lo que implica que los riesgos derivados de su deficiente protección sean a su vez mayores.

III. PROCEDIMIENTO SANCIONADOR PREVISTO 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 (LOPDFPDIE)

III.1. Consideraciones previas

Los cuerpos policiales en el ejercicio de sus funciones, tratan una gran cantidad de información entre la que se incluye diferentes tipos de datos, muchos de los cuales son datos de carácter personal. En este supuesto para su tratamiento se han de tener en cuenta además y entre otros, los preceptos del Código Penal, de la Ley de Enjuiciamiento Criminal, de la Ley de Protección de la Seguridad Ciudadana y la normativa reguladora del derecho a la protección de los datos personales.

Por ello, prevención e investigación criminal y datos personales deben confluir, de manera que se logre la armonía entre el trabajo policial y garantías de derechos a la protección de los datos personales, sin que se menoscabe uno o el otro.

En este sentido ha de entenderse por:

- Prevención o detección delictiva: Prevenir de la comisión de delitos directamente relacionados con los fines indicados en el artículo 3 de la Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana.
- Investigación criminal: las actuaciones dirigidas tanto a la averiguación del delito ya cometido como a la prevención del que trate de cometerse en un futuro, debe entenderse en un sentido amplio que abarque tanto la investigación criminal en sentido estricto como lo que se conoce como inteligencia criminal o información.

Como hemos estudiado, la normativa de protección de datos, en lo que se consideran sus bases fundamentales, es prácticamente la misma en todos los Es-

tados Miembros de la Unión Europea, ya que se trata de leyes internas elaboradas para dar cumplimiento a normas europeas, fiel reflejo de ello son las leyes sobre la materia, como la LOPDGDD y la LOPDP.

La normativa de protección de datos ha tratado de garantizar el derecho fundamental a la privacidad de las personas frente al peligro que supone para este derecho la sociedad de la información, es decir, la posibilidad de acumular, tratar y ceder de forma masiva y con facilidad gran cantidad de datos personales. Con este objetivo las normas comunitarias instauran como bases ineludibles del derecho fundamental a la protección de los datos personales, los principios generales de tratamiento.

A esos principios hay que añadir los derechos de los afectados en este ámbito concreto: acceso, rectificación, supresión y limitación, respecto del tratamiento de los datos de los que son titulares.

Para supervisar el cumplimiento de todos estos principios cada Estado miembro ha determinado su propia Autoridad de Control, en España como ya sabemos se halla la Agencia Española de Protección de Datos o las diferentes Agencias Autonómicas.

Por ello cabe preguntarse, si los diferentes cuerpos policiales, al realizar sus funciones de prevención e investigación del delito deben aplicar todos los principios mencionados de la normativa de protección de datos, es decir si la normativa de protección de datos personales debe aplicarse a rajatabla en el ámbito policial de la investigación criminal o si, por el contrario, deben existir importantes excepciones al régimen jurídico general.

En el ámbito europeo, se consideró que el tratamiento de datos personales por parte de policía implicaba la existencia de un régimen excepcional, como así se recogía ya en el artículo 9.2. del Convenio 108 del Consejo de Europa indicado anteriormente.

La Unión Europea tiene, entre sus objetivos, la creación de un espacio común de Libertad, Seguridad y Justicia, configurado a raíz del Tratado de Maastricht como III Pilar de la Unión, esfera en la cual se sitúa la cooperación policial entre los diferentes Estados Miembros. Por lo tanto, es en el III Pilar en el que se produce el intercambio de información entre cuerpos policiales y la cesión de datos personales con fines de prevención e investigación criminal. Esa necesidad de cooperación policial entre Estados se ha incrementado en los últimos años frente a la amenaza que ha supuesto el terrorismo y la delincuencia organizada.

Con la entrada en vigor de la Ley Orgánica 7/2021 se permite establecen un nivel uniforme y elevado de protección de datos en estas materias para todos los Estados miembros de la UE, lo que facilitando el intercambio de información entre las autoridades competentes y garantiza la eficacia de la cooperación judicial y policial.

Para garantizar el cumplimiento de la citada norma se ha determinado un régimen sancionador que se establece en el Capítulo VIII de la Ley, definiendo los sujetos sobre los que recaerá la responsabilidad, las reglas del concurso de normas para resolver los casos en los que un hecho pueda ser calificado con arreglo a dos o más de ellas, tipo de infracciones y las sanciones que se pueden imponer, fijando asimismo los plazos de prescripción tanto de las infracciones como de las sanciones y de caducidad.

Al estar directamente relacionados con el procedimiento sancionador, deben tenerse en cuenta otros preceptos que, aunque no se hallen dentro de dicho Capítulo VIII, han de considerarse al respecto, tal es el caso de las autoridades de protección de datos art. 48 y ss. o el de las reclamaciones que se regulan en el Capítulo VII.

En este sentido cabe hacer una mención especial al art. 19 donde se regula la posible exigencia de responsabilidad disciplinaria a los miembros de las Fuerzas y Cuerpos de Seguridad en materia de videovigilancia.

Dicho artículo a priori únicamente afectaría a los miembros de las Fuerzas y Cuerpos de Seguridad, quedando excluidos el resto de funcionarios públicos que como autoridades competentes para el tratamiento de datos se indican en el artículo 4 de la Ley.

No obstante, y al margen de que no se recoja la exigencia de responsabilidad disciplinaria para el resto de autoridades competentes dependerá de la regulación que se establezca en sus respectivos regímenes disciplinarios, en aras de determinar si la conducta infractora en el ámbito de la presente ley está o no vinculada con la respectiva norma disciplinaria.

En este sentido cabe señalar que la previsión legal recogida en el artículo 19.2 debería tener su reflejo en las normas disciplinarias de los respectivos cuerpos policiales, al tratarse de unas conductas concretas y específicas, sin que quepa aplicar un tipo genérico en el contexto disciplinario, así y analizando la Ley Orgánica 4/2010, de 20 de mayo, del Régimen disciplinario del Cuerpo Nacional de Policía, no se recogen tales conductas como infracciones, por lo que no sería adecuado aplicar una sanción disciplinaria que no se halle prevista como tal, en consonancia con el principio de tipicidad, principio que tiene una relación directa con el de seguridad jurídica, obligando al legislador a regular dichas infracciones de modo que las normas aplicables permita predecir el tipo y grado de sanción susceptible de ser impuesto, sin que sea posible definir las conductas ilícitas en términos que por su amplitud o vaguedad dejen las mismas en la más absoluta indefinición.

Por lo que concierne al ámbito de la Guardia Civil, la Ley Orgánica 12/2007, de 22 de octubre, del régimen disciplinario de la Guardia Civil, establece en su 7 las siguientes infracciones muy graves:

> *«19. Alterar o manipular los registros de imágenes o sonidos obtenidos con videocámaras.*
>
> *20. Permitir el acceso de personas no autorizadas a las imágenes o sonidos obtenidos por cualquier medio legítimo o utilizar aquéllas o éstos para fines distintos de los previstos legalmente.*
>
> *21. Reproducir las imágenes y sonidos obtenidos con videocámaras para fines distintos de los previstos legalmente.*
>
> *22. Utilizar los medios técnicos regulados en la normativa legal sobre videocámaras para fines distintos de los previstos en ésta.»*

En consecuencia, si coincidieran los distintos aspectos de las conductas infractoras que se recogen en ambos preceptos, podría exigirse la responsabilidad disciplinaria a los miembros de la Guardia Civil, que en tal caso serían los únicos a quienes se exigiría la misma.

El precepto señala dos alternativas al margen de la sanción penal: responsabilidad administrativa *«con sujeción al régimen general de sanciones en materia de protección de datos de carácter personal establecido en esta Ley Orgánica»*, o responsabilidad disciplinaria *«con arreglo al régimen disciplinario correspondiente a los infractores».*

Por el contrario de lo que sucede en la LOPDPGDD, en cuyo artículo 77.3 se puede añadir a la responsabilidad administrativa la responsabilidad disciplinaria en función de la propuesta que en tal sentido haga la autoridad de control que resuelva el expediente: *«Sin perjuicio de lo establecido en el apartado anterior, la autoridad de protección de datos propondrá también la iniciación de actuaciones disciplinarias cuando existan indicios suficientes para ello»*, en la LOPDP se trata de deslindar ambas responsabilidades con la imposición de sanciones en uno u otro sentido.

En este sentido la LOPDP en su artículo 57[16] con el concurso de normas, pretende clarificar la aplicación de la correspondiente norma sancionadora ante la carencia de una regla general a nivel administrativo que resuelva la aplicación de una norma cuando concurra un concurso de leyes, es decir cuando un mismo supuesto de hecho o conducta puede ser subsumidos en dos o más tipos o preceptos de los cuales sólo uno resulta aplicable, a fin de no quebrantar el principio «non bis in ídem» (tal supuesto se da cuando el hecho o conducta es único en su vertiente natural y jurídica, lesionando el mismo bien jurídico, que es protegido por todas las normas concurrentes):

Para determinar la ley aplicable en los supuestos en que concurran varias normas de aplicación sobre la misma conducta infractora, la norma establece los siguientes criterios:

- Criterio de especialidad: *El precepto especial se aplicará con preferencia al general.*
- Criterio de consunción o absorción: *El precepto más amplio o complejo absorberá el que sancione las infracciones subsumidas en aquel.*
- Criterio de gravedad: *En defecto de los criterios anteriores, se aplicará el precepto que sancione los hechos con la sanción mayor.*

La norma establece una excepción en la aplicación de las reglas del concurso cuando los hechos constituyan *«infracciones al Reglamento General de Protección de Datos o a la Ley Orgánica 3/2018, de 5 de diciembre»*, consagrando así la preferencia de estas normas sobre la citada Ley u otras que pudieren concurrir, conformándola así como norma subsidiaria respecto de las anteriores.

[16] LOPDP. *«Artículo 57. Concurso de normas. 1. Los hechos susceptibles de ser calificados con arreglo a dos o más preceptos de esta u otra Ley, siempre que no constituyan infracciones al Reglamento General de Protección de Datos, ni a la Ley Orgánica 3/2018, de 5 de diciembre, se sancionarán observando las siguientes reglas: a) El precepto especial se aplicará con preferencia al general. b) El precepto más amplio o complejo absorberá el que sancione las infracciones subsumidas en aquel. c) En defecto de los criterios anteriores, se aplicará el precepto que sancione los hechos con la sanción mayor. 2. En el caso de que un solo hecho constituya dos o más infracciones, o cuando una de ellas sea medio necesario para cometer la otra, la conducta será sancionada por aquella infracción que conlleve una mayor sanción.*

III.2. Autoridades Competentes

Como se apuntó en el apartado correspondiente, las autoridades independientes de control serían.

- La Agencia Española de Protección de Datos.
- Las autoridades autonómicas de protección de datos, exclusivamente en relación a aquellos tratamientos de los que sean responsables en su ámbito de competencia, y conforme a lo dispuesto en el artículo 57.1 de la Ley Orgánica 3/2018, de 5 de diciembre, y en la normativa autonómica aplicable.

La Agencia Española de Protección de Datos actuará como representante de las autoridades de protección de datos en el Comité Europeo de Protección de Datos.

(Con respecto a las funciones y potestades que ostentan, nos centraremos en aquellas relacionadas con el ámbito de aplicación del procedimiento sancionador).

En cuanto a sus funciones, se pueden enumerar:

- Supervisar y hacer cumplir las disposiciones adoptadas con arreglo a esta Ley Orgánica.
- Promover la sensibilización de los responsables y encargados del tratamiento en relación con las obligaciones que les incumben.
- Facilitar la información solicitada por los interesados sobre el ejercicio de sus derechos en virtud de esta Ley Orgánica y, en su caso, cooperar a tal fin con las autoridades de protección de datos de otros Estados miembros de la Unión Europea.
- Tramitar y responder las reclamaciones presentadas por un interesado o por una entidad, organización o asociación de conformidad con el artículo 55, e investigar, en la medida oportuna, el motivo de la reclamación e informar al reclamante sobre el curso y el resultado de la investigación en un plazo razonable.
- Llevar a cabo investigaciones sobre la aplicación de esta Ley Orgánica, en particular basándose en la información recibida de otra autoridad de protección de datos u otra autoridad pública.
- Las autoridades de protección de datos adoptarán medidas tendentes a facilitar la formulación de las reclamaciones, tales como proporcionar formularios que puedan cumplimentarse electrónicamente, sin excluir otros medios.
- El desempeño de las funciones de las autoridades de control no implicará coste alguno para el interesado ni para el delegado de protección de datos.
- Cuando las solicitudes sean manifiestamente infundadas o excesivas, especialmente debido a su carácter repetitivo, la autoridad de protección de datos podrá negarse a actuar respecto de la solicitud. La carga de la demostración del carácter manifiestamente infundado o excesivo de la solicitud recaerá en la autoridad de protección de datos.

Las potestades de la AEPD, se pueden agrupar en los siguientes grupos:

- De investigación, incluyendo el acceso a todos los datos que estén siendo tratados por el responsable o el encargado del tratamiento, en los términos previstos por la legislación vigente.
- De advertencia y control de lo exigido en esta Ley Orgánica, incluida la sanción de las infracciones cometidas, la elaboración de recomendaciones, órdenes de rectificación, supresión o limitación del tratamiento de datos personales o de limitación temporal o definitiva del tratamiento, incluida su prohibición, así como la orden a los responsables del tratamiento de comunicar las vulneraciones de seguridad de los datos a los interesados.
- De asesoramiento, que comprende la consulta previa prevista en el artículo 36 y la emisión, por propia iniciativa o previa solicitud, de dictámenes destinados a las Cortes Generales o al Gobierno, a otras instituciones u organismos, así como al público en general, acerca de todo asunto relacionado con la protección de datos personales sujeto a esta Ley Orgánica.

Cuando se termine la tramitación parlamentaria urgente del Proyecto de Ley Orgánica por la que se establecen normas que faciliten el uso de información financiera y de otro tipo para la prevención, detección, investigación o enjuiciamiento de infracciones penales, se modificará el artículo 61 de la LO 7/2021, de 26 de mayo, atribuyendo la potsstad sancionadora en las infracciones relativas al deber de colaboración a la Secretaría de Estado de Seguridad y las Delegaciones del Gobierno.

En concreto, el artículo 61.2 dispondrá: "2. En el supuesto de las infracciones recogidas en los artículos 58.j) y 59. j), el ejercicio de la potestad sancionadora corresponderá respectivamente, a las personas titulares de la Secretaría de Estado de Seguridad y de las Delegaciones del Gobierno. Estos procedimientos se regirán por la normativa sobre procedimiento administrativo común de las Administraciones Públicas y el régimen jurídico del sector público, sin perjuicio de las especialidades que se recogen en este capítulo."

III.3. Sujetos responsables (art. 56)

- Los responsables de los tratamientos.
- Los encargados de los tratamientos.

Teniendo en cuenta el ámbito de aplicación de esta Ley, dentro de los anteriores se incluirían las siguientes autoridades competentes:

- Las Fuerzas y Cuerpos de Seguridad.
- Las Administraciones Penitenciarias.
- La Dirección Adjunta de Vigilancia Aduanera de la Agencia Estatal de Administración Tributaria.
- El Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias.

- La Comisión de Vigilancia de Actividades de Financiación del Terrorismo.
- Las Autoridades judiciales del orden jurisdiccional penal
- El Ministerio Fiscal.

- Los representantes de los encargados de los tratamientos no establecidos en el territorio de la Unión Europea (conforme a lo señalado en el artículo 27 del Reglamento).
- El resto de las personas físicas o jurídicas obligadas por el contenido del deber de colaboración establecido en el artículo 7.
  Ese deber de colaboración puede estar motivado por dos supuestos:

  - La solicitud a las Administraciones públicas, como a cualquier persona física o jurídica por las autoridades judiciales, Ministerio Fiscal o la Policía Judicial para que les faciliten los datos, informes, antecedentes y justificantes que sean necesarios para la investigación y enjuiciamiento de infracciones penales o para la ejecución de las penas. Donde la petición de la Policía Judicial se deberá ajustar exclusivamente al ejercicio de las funciones que le encomienda el artículo 549.1 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial y deberá efectuarse siempre de forma motivada, concreta y específica, dando cuenta en todo caso a la autoridad judicial y fiscal.
  - La solicitud a las Administraciones públicas, o a cualquier persona física o jurídica, de datos, informes, antecedentes y justificantes, por las autoridades competentes que los soliciten (las referidas en el art. 4), siempre que estos sean necesarios para el desarrollo específico de sus misiones para la prevención, detección e investigación de infracciones penales y para la prevención y protección frente a un peligro real y grave para la seguridad pública. La petición efectuada deberá ser concreta, específica y motivada conforme a los supuestos expresados.

- El DPD quedaría en todo caso excluido del régimen sancionador establecido en el capítulo VIII de esta Ley.

III.4. Infracciones

Los tipos infractores de la LOPDP vienen establecidos en sus artículos 58 a 60. Dada la trascendencia dentro de este campo los reproducimos y analizamos a continuación:

> *«Artículo 58. Infracciones muy graves.*
> *Son infracciones muy graves:*
> *a) El tratamiento de datos personales que vulnere los principios y garantías establecidos en el artículo 6 o sin que concurra alguna de las condiciones de licitud del tratamiento establecidas en el artículo 11, siempre que se causen perjuicios de carácter muy grave a los interesados.*
> *b) El acceso, cesión, alteración y divulgación de los datos al margen de los supuestos autorizados por el responsable o encargado de los datos, siempre que no constituya ilícito penal.*

c) La transferencia temporal o definitiva de datos de carácter personal con destino a Estados que no sean miembros de la Unión Europea o a destinatarios que no sean autoridades competentes, establecidos en dichos Estados incumpliendo las condiciones previstas en los artículos 43 y 47.

d) La utilización de los datos para una finalidad que no sea compatible con el objetivo para el que fueron recogidos o cuando no se cumplan las condiciones establecidas en el artículo 6, siempre que no se cuente con una base legal para ello.

e) El tratamiento de datos personales de las categorías especiales sin que concurra alguna de las circunstancias previstas en el artículo 13 o sin garantizar las medidas de seguridad adecuadas, que cause perjuicios graves a los interesados.

f) La omisión del deber de informar al interesado acerca del tratamiento de sus datos de carácter personal conforme a lo dispuesto en esta Ley Orgánica.

g) La vulneración del deber de confidencialidad del encargado del tratamiento, establecido en el artículo 30.

h) La adopción de decisiones individuales automatizadas sin las garantías señaladas en el artículo 14, siempre que se causen perjuicios de carácter muy grave para los interesados.

i) El impedimento, la obstaculización o la falta de atención reiterada del ejercicio de los derechos del interesado de acceso, rectificación, supresión de sus datos o limitación del tratamiento, siempre que se causen perjuicios de carácter muy grave para los interesados.

j) La negativa a proporcionar a las autoridades competentes la información necesaria para la prevención, detección, investigación y enjuiciamiento de infracciones penales, para la ejecución de sanciones penales o para la protección y prevención frente a las amenazas contra la seguridad pública de acuerdo con lo previsto en el artículo 7, así como a informar al interesado cuando se comuniquen sus datos en virtud del deber de colaboración establecido en dicho artículo.

k) La resistencia u obstrucción del ejercicio de la función inspectora de las autoridades de protección de datos competentes.

l) La falta de notificación a las autoridades de protección de datos competentes acerca de una violación de la seguridad de los datos personales, cuando sea exigible, así como la ausencia de comunicación al interesado de una violación de la seguridad cuando sea procedente de acuerdo con el artículo 39, siempre que se deriven perjuicios de carácter muy grave para el interesado.

m) El incumplimiento de las resoluciones dictadas por las autoridades de protección de datos competentes, en el ejercicio de las potestades que le confiere el artículo 50.

n) No facilitar el acceso del personal de las autoridades de protección de datos competentes a los datos personales, información, locales, equipos y medios de tratamiento, cuando sean requeridos por las mismas, en el ejercicio de sus poderes de investigación.

ñ) El incumplimiento de los plazos de conservación y revisión establecidos en virtud del artículo 8.

Dentro del cuatro de las infracciones muy graves vamos a analizar las siguientes conductas:

«a) El tratamiento de datos personales que vulnere los principios y garantías establecidos en el artículo 6 o sin que concurra alguna de las condiciones

de licitud del tratamiento establecidas en el artículo 11, siempre que se causen perjuicios de carácter muy grave a los interesados».

La vulneración de los principios a que se refiere dicho precepto durante el tratamiento de los datos cuando, constituyéndose como las bases permanentes donde se debe apoyar el sujeto activo, se cause un resultado dañino de carácter muy grave al interesado conforma los elementos del tipo de esta infracción.

«b) El acceso, cesión, alteración y divulgación de los datos al margen de los supuestos autorizados por el responsable o encargado de los datos, siempre que no constituya ilícito penal».

La finalidad, se configura como principio fundamental en el tratamiento de los datos, por ello, en cualquier fase o uso que se haga de los mismos, debe estar adecuado y en consonancia con la finalidad para la que se han obtenido. Así y sin perjuicio de lo reseñado al respecto en otros preceptos, debemos considerar que el mero acceso a los datos, al margen de las circunstancias establecidas por el responsable o encargado de los mismos, que no son otras que las finalidades que se establecen en el artículo 1 de la Ley: *«... prevención, detección, investigación y enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y prevención frente a las amenazas contra la seguridad pública»,* se considera una infracción muy grave, salvo que dicho acceso sea constitutivo de un ilícito penal.

Por ello el acceso de datos personales deberá estar acreditado y fundamentado conforme a los citados fines.

Ello no debe implicar que el mero acceso a los datos implique una estricta aplicación de la norma, debiendo considerarse otros criterios que cualifiquen dicha conducta como infracción muy grave o delito, tal es el caso del perjuicio que con ello se pueda originar al sujeto titular de los mismos, o si el acceso se ha producido a datos considerados «sensibles» lo que constituiría un perjuicio en sí (ej. STS 1153/2021).

«Artículo 59. Infracciones graves.

Son infracciones graves:

a) El tratamiento de los datos de carácter personal cuando se incumplan los principios del artículo 6 o las condiciones de licitud del tratamiento del artículo 11, siempre que no constituya una infracción muy grave.

b) El tratamiento de datos personales de las categorías especiales sin que concurra alguna de las circunstancias previstas en el artículo 13 o sin garantizar las medidas de seguridad adecuadas, siempre que no constituya una infracción muy grave.

c) La adopción de decisiones individuales automatizadas sin las garantías señaladas en el artículo 14, siempre que no constituya una infracción muy grave.

d) La falta de designación de un delegado de protección de datos en los términos previstos en el artículo 40 o no posibilitar la efectiva participación del mismo en todas las cuestiones relativas a la protección de datos personales, no respaldarlo o interferir en el desempeño de sus funciones.

e) El incumplimiento de la puesta a disposición al interesado de la información prevista en el artículo 21 o del deber de comunicación al mismo, o a la autoridad de protección de datos competente, de una violación de la seguridad de los datos, que entrañe un grave perjuicio para los derechos y libertades del interesado.

f) La ausencia de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para aplicar de forma efectiva los principios de protección de datos, incluidas las medidas oportunas desde el diseño y por defecto, así como para integrar las garantías necesarias en el tratamiento.

g) El impedimento, la falta de atención o la obstaculización de los derechos del interesado de acceso, rectificación, supresión de sus datos o limitación del tratamiento, siempre que no constituya infracción muy grave.

h) El incumplimiento de la obligación de llevanza de los registros de actividades de tratamiento o del registro de operaciones de tratamiento, si se causan perjuicios de carácter grave a los interesados.

i) El incumplimiento de las estipulaciones recogidas en el contrato u acto jurídico que vincula al responsable y al encargado del tratamiento, salvo en los supuestos en que fuese necesario para evitar la infracción de la legislación en materia de protección de datos y se hubiese advertido de ello al responsable o al encargado del tratamiento, así como el incumplimiento de las obligaciones impuestas en el artículo 30.

j) La falta de colaboración diligente con las autoridades competentes en el cumplimiento de las obligaciones establecidas en el artículo 7, cuando no constituya una infracción muy grave.

k) La falta de cooperación, la actuación negligente o el impedimento de la función inspectora de las autoridades de protección de datos competentes, cuando no constituya infracción muy grave.

l) El incumplimiento de la evaluación de impacto en la protección de los datos de carácter personal, si se derivan perjuicios o riesgos de carácter grave para los interesados.

m) El tratamiento de datos personales sin haber consultado previamente a la autoridad de protección de datos competente, en los casos en que dicha consulta resulte preceptiva conforme al artículo 36.

Artículo 60. Infracciones leves.

Son infracciones leves:

a) La afectación leve de los derechos de los interesados como consecuencia de la ausencia de la debida diligencia o del carácter inadecuado o insuficiente de las medidas técnicas y organizativas que se hubiesen implantado.

b) El incumplimiento del principio de transparencia de la información o del derecho de información del interesado establecido en el artículo 21 cuando no se facilite toda la información exigida en esta Ley Orgánica.

c) La inobservancia de la obligación de informar al interesado y a los destinatarios a los que se hayan comunicado o de los que procedan los datos personales rectificados, suprimidos o respecto de los que se haya limitado el tratamiento, conforme a lo establecido en el artículo 23.

d) El incumplimiento de la llevanza de registros de actividades de tratamiento o del registro de operaciones o que los mismos no incorporen toda la información exigida legalmente, siempre que no constituya infracción grave.

e) El incumplimiento de la obligación de suprimir los datos referidos a una persona fallecida cuando fuera exigible legalmente.

f) La falta de formalización por los corresponsables del tratamiento del acuerdo que determine las obligaciones, funciones y responsabilidades respectivas, a propósito del tratamiento de datos personales y de sus relaciones con los interesados, así como la inexactitud o la falta de concreción en la determinación de las mismas.

g) El incumplimiento de la obligación del encargado del tratamiento de informar al responsable del tratamiento acerca de una posible infracción de las disposiciones de esta Ley Orgánica, como consecuencia de una instrucción recibida de este.

h) La notificación incompleta o defectuosa a la autoridad de protección de datos competente de la información relacionada con una violación de seguridad de los datos personales, el incumplimiento de la obligación de documentarla o del deber de comunicar al interesado su existencia, cuando no constituya una infracción grave.

i) La aportación de información inexacta o incompleta a la autoridad de protección de datos competente, en los supuestos en los que el responsable del tratamiento deba elevarle una consulta previa.

j) La falta de publicación de los datos de contacto del delegado de protección de datos, o la ausencia de comunicación de su designación y cese a la autoridad de protección de datos competente, de conformidad con el artículo 40, cuando su nombramiento sea exigible de acuerdo con esta Ley Orgánica.»

III.5. Sanciones

Por la comisión de las infracciones tipificadas en la LOPDP se impondrán las siguientes sanciones:

En caso de que el sujeto responsable sea algunos de los enumerados en el artículo 77.1 de la LOPDP, se impondrán las sanciones y se adoptarán las medidas establecidas en dicho artículo.

Cuando el sujeto infractor sea distinto de los señalados anteriormente, podrá ser sancionado, con multa de la siguiente cuantía:

a) Las infracciones muy graves, con multa de 360.001 a 1.000.000 euros.
b) Las infracciones graves, con multa de 60.001 a 360.000 euros.
c) Las leves, con multa de 6.000 a 60.000 euros.

A efectos de la determinación de la cuantía de la sanción, se tendrán en cuenta los criterios establecidos en el artículo 83.2 del RGPD y en el artículo 76.2 de la LOPDGDD.

En cuando a las sanciones cabe destacar la reducción de su cuantía respecto a las previstas en la LOPDGDD, siendo aplicables los criterios de proporcionalidad que se establecen en el art. 76 1 y 2 de la misma.

III.6. Reclamaciones

Cuando los interesados aprecien que el tratamiento de los datos personales haya infringido las disposiciones de esta Ley Orgánica o no haya sido atendida su solicitud de ejercicio de los derechos reconocidos en los artículos 21, 22 y 23 tendrán derecho a presentar una reclamación ante la autoridad de protección de datos.

Dichas reclamaciones serán tramitadas por la autoridad de protección de datos competente con sujeción al procedimiento establecido en el título VIII de la LOPDGDD, por lo cual se aplican las mismas reglas anteriormente expuestas para la presentación de reclamaciones, con algunas salvedades dadas por la interven-

ción de otros actores en atención a las especificas finalidades que se persiguen con la presente norma:

- Los interesados tendrán derecho a ser indemnizados por el responsable del tratamiento, o por el encargado del tratamiento cuando formen parte del sector público, en el caso de que sufran daño o lesión en sus bienes o derechos como consecuencia del incumplimiento de lo dispuesto en esta Ley Orgánica.
- También se establece la indemnización cuando el encargado del tratamiento no forme parte del sector público; en tal caso se regirán por el régimen de responsabilidad del contratista (responsable del tratamiento) por los daños causados a terceros regulado en la normativa sobre contratos del sector público.

Cuando los daños y perjuicios hayan sido ocasionados como consecuencia inmediata y directa de una orden de la autoridad competente responsable del tratamiento, será esta la responsable.

Sin perjuicio de cualquier otro recurso administrativo o reclamación, toda persona física o jurídica tendrá derecho a recurrir ante la jurisdicción contencioso-administrativa, contra los actos y resoluciones dictadas por la autoridad de protección de datos competente.

El interesado podrá conferir su representación a una entidad, organización o asociación sin ánimo de lucro que haya sido correctamente constituida, cuyos objetivos estatutarios sean de interés público y que actúe en el ámbito de la protección de los derechos y libertades de los interesados en materia de protección de sus datos personales, para que ejerza los derechos antes señalados.

El ejercicio de la potestad sancionadora, que corresponde a las Autoridades de protección de datos competentes, se regirá por lo dispuesto en el presente Capítulo, por los títulos VII y IX de la LOPDGDD, y, en cuanto no las contradigan, con carácter supletorio, por la normativa sobre procedimiento administrativo común de las Administraciones públicas y el régimen jurídico del sector público.

III.7. Prescripción de las infracciones y sanciones (art. 63)

- En el caso de las infracciones, tras su comisión el plazo que establece la ley para evitar su castigo por haber transcurrido el plazo para su prescripción:

  - Muy graves: tres años
  - Graves: dos años.
  - Leves: seis meses.

Interrumpirá la prescripción la iniciación, con conocimiento del interesado, del procedimiento sancionador, reiniciándose el plazo de prescripción si el expediente sancionador estuviere paralizado durante más de seis meses por causas no imputables al presunto infractor.

Se interrumpirá igualmente la prescripción como consecuencia de la apertura de un procedimiento judicial penal, hasta que la autoridad judicial comunique al órgano administrativo su finalización.

- Por lo que respecta a la prescripción de las sanciones, los plazos son los siguientes:
  - Sanciones por infracciones muy graves: tres años.
  - Sanciones por infracciones graves: dos años
  - Sanciones por infracciones leves: un año

Computados desde el día siguiente a aquel en que adquiera firmeza en vía administrativa la resolución por la que se impone la sanción.

III.8. Plazo de caducidad del expediente sancionador (art. 64)

Iniciado un procedimiento sancionador por alguna de las infracciones previstas en la LOPDP, el mismo caducará transcurridos seis meses desde su incoación sin que se haya notificado la resolución, salvo que se haya paralizado por causas imputables al interesado, o se hubiere suspendido por prejudicialidad penal (existencia de un procedimiento judicial penal, en el que concurra identidad de sujeto, hecho y fundamento).

Aunque el procedimiento hubiere caducado ello no implica que el mismo finalice, y el expedientado quede exento de responsabilidad, puesto que en tanto no haya prescrito la infracción se puede acordar la incoación de un nuevo procedimiento por parte de la administración.

También ha de tenerse en cuenta que los procedimientos caducados no interrumpen el plazo de prescripción.

Ej. Se inicia un expediente por infracción grave prevista en el art. 59.a) de la citada Ley, se dicta resolución y se notifica la misma a los 10 meses de su comisión, ¿Qué ocurrirá con el expediente, ha prescrito, ha caducado, se puede iniciar uno nuevo? El expediente ha caducado por al no haber prescrito la infracción se puede iniciar un nuevo expediente, previo archivo del anterior.

- Si iniciado ese nuevo expediente se dicta y notifica resolución sancionadora a los 8 meses.

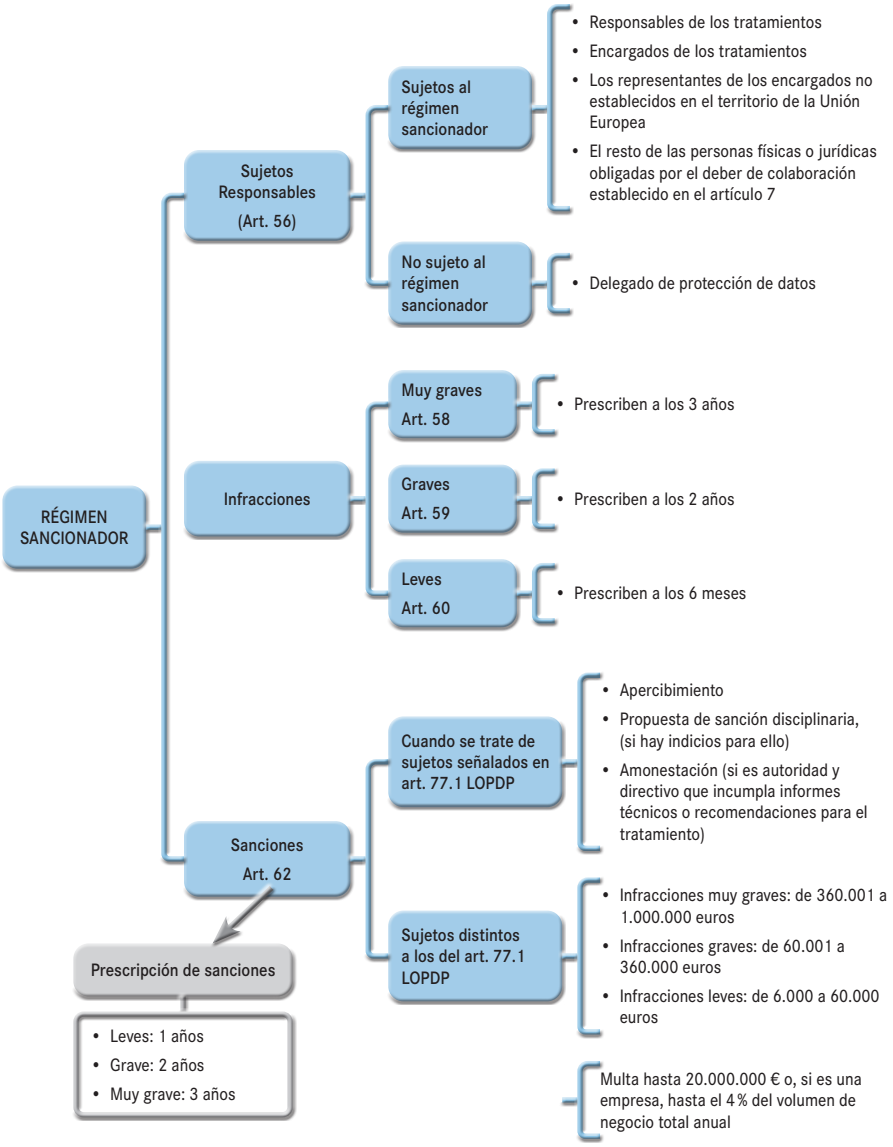
¿Ha prescrito la infracción por haber pasado más de un año desde que se cometió la misma?

Al incoarse un nuevo expediente dentro del plazo de prescripción, la misma queda interrumpida por lo que no entra en juego.

¿Qué ocurriría si la resolución se dicta y notifica a los 9 meses y un día?

Ha transcurrido el plazo de caducidad, por lo que entra en juego la prescripción, de manera que dicha caducidad permite que el expediente prescriba, sin que se interrumpa por ello.

III.9. Cuadro resumen de la LOPDP



Artículo 65. Carácter subsidiario del procedimiento administrativo sancionador respecto del penal.

1. No podrán sancionarse los hechos que hayan sido sancionados penal o administrativamente cuando se aprecie identidad de sujeto, de hecho y de fundamento.

2. En los supuestos en que las conductas pudieran ser constitutivas de delito, el órgano administrativo pasará el tanto de culpa a la autoridad judicial o al Ministerio Fiscal y se abstendrá de seguir el procedimiento sancionador mientras la autoridad judicial no dicte sentencia firme o resolución que de otro modo ponga fin al procedimiento penal, o el Ministerio Fiscal no acuerde la improcedencia de iniciar o proseguir las actuaciones en vía penal, quedando hasta entonces interrumpido el plazo de prescripción.

La autoridad judicial y el Ministerio Fiscal comunicarán al órgano administrativo la resolución o acuerdo que hubieran adoptado.

3. De no haberse estimado la existencia de ilícito penal, o en el caso de haberse dictado resolución de otro tipo que ponga fin al procedimiento penal, podrá iniciarse o proseguir el procedimiento sancionador. En todo caso, el órgano administrativo quedará vinculado por los hechos declarados probados en vía judicial.

4. Las medidas cautelares adoptadas antes de la intervención judicial podrán mantenerse mientras la autoridad judicial no resuelva otra cosa).

III.10. Subordinación del procedimiento administrativo al procedimiento penal

Por último, hacer referencia a lo dispuesto por el artículo 65, donde se determina el carácter subsidiario del procedimiento administrativo sancionador respecto del penal.

En dicho precepto al igual que se expone en el mismo sentido por otras normas (artículo 45 de la LOPSC) se determina la preferencia del orden jurisdiccional penal sobre el administrativo, en consonancia con el principio «non bis in ídem», tal como se concibe por la jurisprudencia (STC 188/2005) y se plasma en el derecho positivo (arts. 31 LRJSP y 77.4 LPACAP).

Para la concurrencia de sanciones penales o administrativas debe existir la triple identidad: subjetiva (el sujeto afectado debe ser el mismo), fáctica (que los hechos objeto de la infracción o del delito sean los mismos) fundamento (los bienes jurídicos protegidos por la norma han de coincidir), como ha quedado expuesto en el tema anterior, de manera que la ausencia de uno de ellos justificaría la aplicación de otra sanción con independencia de su naturaleza.

Previamente a la imposición de la correspondiente sanción y con objeto de garantizar el citado principio, cuando los órganos de la AEPD que se hallen tramitando un procedimiento sancionador por presunta infracción a la normativa sobre protección de datos personales, aprecien que los hechos pudieren ser constitutivos de delito, deberán remitir las actuaciones a la autoridad judicial o al Ministerio Fiscal, dada la preeminencia de la jurisdicción penal sobre potestad administrativa, acordando la suspensión del expediente administrativo hasta que la autoridad judicial no dicte sentencia firme o resolución que ponga fin al procedimiento penal, o el Ministerio Fiscal no acuerde la improcedencia de iniciar o

proseguir las actuaciones en vía penal, quedando entre tanto interrumpido el plazo de prescripción de la correspondiente infracción.

Esa subordinación de los procedimiento administrativos frente a los penales, conlleva que los órganos administrativos queden vinculados por la resolución judicial, de manera que si a resultas del procedimiento penal se aprecia que la conducta es constitutiva de delito, la AEPD deberá dictar resolución archivando el procedimiento administrativo sancionador sin declaración de responsabilidad en tal ámbito para el interesado, o no proceder a su inicio en caso de que aún no se acordado su incoación, no obstante cuando no se aprecie ilícito penal, o se dicte resolución de otro tipo que ponga fin al procedimiento penal, la autoridad administrativa podrá iniciar el correspondiente expediente sancionador o reabrir las actuaciones que habían quedado suspendidas a expensas del dictamen judicial.

ABREVITURAS UTILIZADAS

AEPD: Agencia Española de Protección de Datos

APP's: Aplicaciones. Del inglés: *«Application»*.

Art.: Artículo.

BDSN: Base de Datos de Señalamientos Nacionales.

CC: Código Civil.

CCTV: Circuito Cerrado de Televisión.

CE: Constitución Española

CEDH: Carta Europea de los Derechos Humanos

CEPD: Comité Europeo de Protección de Datos.

CITCO: Centro de Inteligencia contra el Terrorismo y el Crimen Organizado.

CP: Código Penal.

DDFIN: Directiva (UE) 2019/1153 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, por la que se establecen normas destinadas a facilitar el uso de información financiera y de otro tipo para la prevención, detección, investigación o enjuiciamiento de infracciones penales y por la que se deroga la Decisión 2000/642/JAI del Consejo.

DDP: 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 y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.

DPD: Delegado de Protección de Datos

DPNR: Directiva (UE) 2016/681 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la utilización de datos del registro de nombres de los pasajeros (PNR) para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave.

DEJ: Diccionario del Español Jurídico.

DRAE: Diccionario de la Real Academia Española.

ECRIS: Sistema Europeo de Información de Antecedentes Penales

EES: Sistema de Entrada y Salida

Ej.: Por ejemplo.

EPRIS: Sistema Europeo de Índice de Ficheros Policiales

EIPD: Evaluación Impacto de Protección de Datos

ETIAS: Sistema Europeo de Información y Autorización de Viajes (ETIAS).

FCS: Fuerzas y Cuerpos de Seguridad

LECRIM: Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal.

LOFCS: Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad.

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

LOPD: Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

LOPDGDD: Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

LOPDFIN: Ley Orgánica por la que se establecen normas que faciliten el uso de información financiera y de otro tipo para la prevención, detección, investigación o enjuiciamiento de infracciones penales.

LOPNR: Ley Orgánica 1/2020, de 16 de septiembre, sobre la utilización de los datos del Registro de Nombres de Pasajeros para la prevención, detección, investigación y enjuiciamiento de delitos de terrorismo y delitos graves.

LOPSC: Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana

LOVV: Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos.

LRJSP: Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

LSO: Ley 9/1968, de 5 de abril, sobre secretos oficiales.

LSP: Ley 5/2014, de 4 de abril, de Seguridad Privada.

OCDE: Organización para la Cooperación y el Desarrollo Económicos

Págs.: Páginas

PIA: Privacy Impact Assessment

RAE: Real Academia Española

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 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.

RLOPD: 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.

RLVV: Real Decreto 596/1999, de 16 de abril, por el que se aprueba el Reglamento de desarrollo y ejecución de la Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos.

SEPD: Supervisor Europeo de Protección de Datos

SIS-II: Sistema de Información Schengen de segunda generación

SOA: Declaración de Aplicabilidad

STC: Sentencia del Tribunal Constitucional

STS: Sentencias del Tribunal Supremo

TC: Tribunal Constitucional

TEDH: Tribunal Europeo de Derechos Humanos

TIA: Transfer Impact Assessment

TIC's: Tecnologías de la Información y Comunicación.

TS: Tribunal Supremo

TJUE: Tribunal de Justicia de la Unión Europea.

Vgr.: Verbigracia. Por ejemplo.

VIS: Sistema de Información de Visas

WP29: Article 29 Working Party

BIBLIOGRAFÍA-WEBGRAFÍA

- ARNALDO ALCUBILLA, E, GONZÁLEZ-TREVIJANO SÁNCHEZ, P, «Constitución y Derechos Fundamentales» ISBN. 978-84-8126-268-1. Ed. La Ley.
- ARZOZ SANTISTEBAN, X *«Videovigilancia y derechos fundamentales: análisis de la constitucionalidad de la Ley Orgánica 4/1997»*, Revista Española de Derecho Constitucional.
- DE LA SERNA BILBAO. M.N. *«Seguridad ciudadana y los sistemas de videovigilancia. Límites, garantías y regulación.»*
- FERNÁNDEZ GONZÁLEZ. C.M, AYLLÓN SANTIAGO, H. S. Prólogo: Jorge Álvaro NAVAS ELORZA «Tratamiento de datos de carácter personal en el ámbito policial» ISBN: 978-84-290-2433-3 Editorial Reus. 1ª Edición.
- FERNÁNDEZ SÁNCHEZ. P *«Intereses y críticas sobre el uso de bodycam": El uso policial de las bodycam y sus propuestas de mejora.»*
- LASCURAÍN SÁNCHEZ. J.A. y otros. *«Manual de Introducción al Derecho Penal» ISBN: 978-84-340-2591-2. Editorial. AEBOE. 2019.*
- MARCOS AYJÓN. M. «La protección de datos de carácter personal en la Justicia penal: 10» 978-8412157932 Colección Penal J.M. Bosch Editor. 1ª Edición.
- MARCOS AYJON, M. *«La nueva Ley Orgánica para la protección de datos personales en la prevención, investigación, enjuiciamiento de delitos y ejecución de penas.»* Diario la ley. Junio 2021. Wolters Kluwer.
- PACHECO TORRALVA.A, NAVARRO GOZALVES, A. DE BARTOLOME CENZANO, J.C. «La Actuación Policial en la diversidad social y cultural. Buenas Práctica ante el Racismo, la Xenofobia y la Discriminación» ISBN. 978-84-9143-088-9. Editorial Tirant lo Blanch.
- PAU. A. y HERNANDO GRANDE.A *«La Cibercosmología como premisa del Ciberderecho»* Boletín del Ministerio de Justicia. Nº 2236. Año LXXV. Enero de 2021. NIPO.051-15-001-5
- POLO ROCA, A. *«Datos, Datos, Datos: El dato personal, el dato no personal, el dato personal compuesto, la anonimización, la pertenencia del dato y otras cuestiones sobre datos.»* Universidad de Deusto • ISSN 0423-4847 Videovigilancia y protección de datos Especial referencia a la grabación de la vía pública desde el espacio privado, publicado por Wolters Kluwer.
- VILLANUEVA TURNES. A. *«La videovigilancia en lugares públicos por razones de seguridad: autorización y principios.»*
- Informe de la Abogacía del Estado de Madrid de fecha 7 de mayo de 2018 sobre las dudas planteadas por la Comisión de Garantías de la Videovigilancia en relación con la aplicación de la LOV cuando las cámaras se incorporan a drones.
- ISSN-e 2386-9062, Vol. 69/1, enero-junio 2021, págs. 211-240 http://www.revista-estudios.deusto.es/Carta de Derechos Fundamentales de la Unión Europea (https://www.europarl.europa.eu/charter/pdf/text_es.pdf)
- Tratado de Funcionamiento de la Unión Europea (https://www.boe.es/doue/2010/083/Z00047-00199.pdf)

- Tratado de la Unión Europea (https://www.boe.es/doue/2010/083/Z00013-00046.pdf)
- 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 (UE) 2018/1860 del Parlamento Europeo y del Consejo, de 28 de noviembre de 2018, sobre la utilización del Sistema de Información de Schengen para el retorno de nacionales de terceros países en situación irregular.
- Reglamento (UE) 2018/1861 del Parlamento Europeo y del Consejo, de 28 de noviembre de 2018, relativo al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen (SIS) en el ámbito de las inspecciones fronterizas, por el que se modifica el Convenio de aplicación del Acuerdo de Schengen y se modifica y deroga el Reglamento (CE) n.° 1987/2006.
- Reglamento (UE) 2018/1862 del Parlamento Europeo y del Consejo, de 28 de noviembre de 2018, relativo al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen (SIS) en el ámbito de la cooperación policial y de la cooperación judicial en materia penal, por el que se modifica y deroga la Decisión 2007/533/JAI del Consejo, y se derogan el Reglamento (CE) Nº 1986/2006 del Parlamento Europeo y del Consejo y la Decisión 2010/261/UE de la Comisión.
- Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) 45/2001 y la Decisión 1247/2002/CE.
- Reglamento (UE) 2019/817 del Parlamento Europeo y del Consejo, de 20 de mayo de 2019, relativo al establecimiento de un marco para la interoperabilidad de los sistemas de información de la UE en el ámbito de las fronteras y los visados y por el que se modifican los Reglamentos (CE) 767/2008, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 y (UE) 2018/1861 del Parlamento Europeo y del Consejo, y las Decisiones 2004/512/CE y 2008/633/JAI del Consejo.
- Reglamento (UE) 2019/818 del Parlamento Europeo y del Consejo, de 20 de mayo de 2019, relativo al establecimiento de un marco para la interoperabilidad entre los sistemas de información de la UE en el ámbito de la cooperación policial y judicial, el asilo y la migración y por el que se modifican los Reglamentos (UE) 2018/1726, (UE) 2018/1862 y (UE) 2019/816.
- 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.
- Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y la libre circulación de dichos datos, y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.
- Directiva (UE) 2016/681 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la utilización de datos del registro de nombres de los pasajeros (PNR) para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave.
- Directiva (UE) 2019/1153 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, por la que se establecen normas destinadas a facilitar el uso de información financiera y de otro tipo para la prevención, detección, investigación o enjuiciamiento de infracciones penales y por la que se deroga la Decisión 2000/642/JAI del Consejo.

- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
- Ley Orgánica 4/2000, de 11 de enero, sobre derechos y libertades de los extranjeros en España y su integración social.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Ley Orgánica 1/2020, de 16 de septiembre, sobre la utilización de los datos del Registro de Nombres de Pasajeros para la prevención, detección, investigación y enjuiciamiento de delitos de terrorismo y delitos graves.
- 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 2/1986, de 13 marzo, de Fuerzas y Cuerpos de Seguridad.
- Ley Orgánica 12/2007, de 22 de octubre, del régimen disciplinario de la Guardia Civil.
- Ley Orgánica 4/2010, de 20 de mayo, del Régimen disciplinario del Cuerpo Nacional de Policía.
- Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal
- Anteproyecto de Ley Orgánica por la que se establecen normas que faciliten el uso de información financiera y de otro tipo para la prevención, detección, investigación o enjuiciamiento de infraccione penales, por el que se transpone la Directiva (UE) 2019/1153 del Parlamento Europeo y del Consejo, de 20 de junio de 2019.
- Real Decreto de 14 de septiembre de 1882, por el que se aprueba la Ley de Enjuiciamiento Criminal.
- Ley 9/1968, de 5 de abril, sobre secretos oficiales.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y derechos y obligaciones en materia de información y documentación clínica.
- Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias
- Real Decreto-ley 5/2018, de 27 de julio, de medidas urgentes para la adaptación del Derecho español a la normativa de la Unión Europea en materia de protección de datos.
- Decreto 242/1969, de 20 de febrero, por el que se desarrollan las disposiciones de la Ley 9/1968, de 5 de abril, sobre secretos oficiales.
- Normas de la Autoridad Nacional para la Protección de la Información Clasificada. Autoridad Delegada para la Seguridad de la información Clasificada (Oficina Nacional de Seguridad). Ministerio de Defensa. Guía para el cumplimiento del deber de informar, editada por la Agencia Española de Protección de Datos, la Agencia Catalana de protección de datos y la Agencia Vasca de Protección de Datos.
- Guía para la notificación de brechas de datos personales, elaborada por la Agencia Española de Protección de Datos en junio de 2021.
- Guía sobre el uso de videocámaras para seguridad y otras finalidades. Agencia Española de Protección de Datos.
- Guía tratamiento de datos en el ámbito local AEPD 2021.
- Protección de datos: guía para el ciudadano, elaborada por la Agencia Española de Protección de Datos.
- Guidelines 01/2021 «on Examples regarding Data Breach Notification» adoptadas el 14 de diciembre de 2021.
- Guidelines 01/2022 on data subject rights - Right of access.
- Directrices sobre notificación de brechas de datos personales de acuerdo con el Reglamento 2016/679 (WP250), adoptadas el 3 de octubre de 2017 por el Grupo de Trabajo

del Artículo 29 y refrendado en la primera reunión del Comité Europeo de Protección de Datos.
- UNE-EN ISO/IEC 27001:2017. Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos.
- UNE-EN ISO/IEC 27002:2017. Tecnología de la Información. Técnicas de seguridad. Código de prácticas para los controles de seguridad de la información
- ISO/IEC 29100:2011 Information technology – Security Techniques – Privacy framework
- Guía Nacional de notificación y gestión de ciberincidentes. DSN.
- Guía CCN-STIC 817 de Gestión de ciberincidentes en el ámbito del ENS. CCN- CERT
- http://www.interior.gob.es/web/servicios-al-ciudadano/cancelacion-de-antecedentes-policiales/procedimiento
- http://www.interior.gob.es/web/servicios-al-ciudadano/participacion-ciudadana/proteccion-de-datos-de-caracter-personal/tutela-de-los-derechos#normativa
- https://www.aepd.es/es/internacional/supervision-de-grandes-sistemas/sistema-de-informacion-schengen-sis
- https://rafaeljimenezasensio.com/2018/05/23/la-regulacion-europea-de-proteccion-de-datos-de-la-directiva-al-rgpd/
- https://www.ugr.es/~redce/REDCE4/articulos/12guerrero.htm
- https://www.aepd.es/es
- https://edpb.europa.eu/about-edpb/about-edpb_es
- https://edps.europa.eu/_en?lang=es
- https://www.europeandataportal.eu/es
- https://data.europa.eu/euodp/es/data/
- https://iapp.org/lang/es/
- https://apdcat.gencat.cat/es/inici/
- https://www.avpd.euskadi.eus/s04-5213/es/
- https://www.ctpdandalucia.es/
- https://www.ccn.cni.es/index.php/es/menu-ccn-es
- https://www.ccn.cni.es/index.php/es/menu-ccn-es/oficina-nacional-de-seguridad-ons
- http://www.oas.org/es/sla/ddi/proteccion_datos_personales_otros_documentos.asp
- https://www.acnur.org/fileadmin/Documentos/Publicaciones/2016/10909.pdf
- https://www.congreso.es/web/guest/proyectos-de-ley?p_p_id=iniciativas&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view&_iniciativas_mode=mostrarDetalle&_iniciativas_legislatura=XIV&_iniciativas_id=121%2F000046
- https://www.consilium.europa.eu/es/policies/data-protection-reform/data-protection-law-enforcement/#:~:text=La%20especificidad%20de%20las%20actividades,Estados%20miembros%20en%20estos%20%C3%A1mbitos.
- https://blogs.uspceu.es/mundo-juridico/la-protecci%C3%B3n-de-datos-en-el-%C3%A1mbito-policial-fase-transitoria
- Protección de datos en el ámbito policial (05/03/2020), Carlos Manuel Fernández González (USPCEU)
- http://help.elearning.ext.coe.int

«Cuando se habla del Derecho a la Protección de Datos Personales en un marco técnico o teórico, inmediatamente la gran mayoría de los actores piensan en el Reglamento General de Protección de Datos y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. No obstante, este ámbito del Derecho no acaba ni mucho menos con estos instrumentos; otro gran bloque normativo regula la actuación de las autoridades competentes y de los propios interesados cuando la finalidad de los tratamientos de los datos es la prevención, detección, investigación y enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluidas la protección y prevención frente a las amenazas contra la seguridad pública.

El conocimiento del contenido de éstas disposiciones legales especiales y de las modificaciones introducidas en la normativa procesal penal, en la policial y en la penitenciaria, es una cuestión fundamental para que, todos los sujetos involucrados en estos ámbitos, garanticen la protección los datos personales de los interesados durante el desarrollo de sus misiones y faciliten el ejercicio de sus derechos.

Cuestiones como qué normativa se aplica en cada momento, cuáles son los conceptos básicos, quiénes son las autoridades competentes, qué tipos de exclusiones de aplicación existen, las distintas categorías de interesados, el deber de colaboración, especialidades en el ejercicio de los derechos o el uso de dispositivos de captación de imágenes y/o sonidos, son algunos de los aspectos que se recogen en esta monografía y sobre los cuales se pretende arrojar la mayor claridad expositiva e interpretativa.

Los autores, profesionales que han participado y participan en el desarrollo nacional e internacional de la normativa de protección de datos en este marco, han realizado en esta obra un ejercicio de síntesis con el ánimo de conformar un elemento de apoyo para el estudio y la consulta por parte de todos aquellos que en su día a día tratan datos personales en este campo.»

ISBN 978-84-8150-335-7
9 788481 503357

GOBIERNO DE ESPAÑA
MINISTERIO DEL INTERIOR