Región de Murcia

ESCUELA DE FORMACIÓN E INNOVACIÓN ADMINISTRACIÓN PÚBLICA

Cuerpo Administrativo. Turno de Promoción Interna

TEMA 8

La protección de datos de carácter personal: Disposiciones generales. Datos especialmente protegidos.

Autora: Sofía Driéguez Moreno
Actualiza: Gloria Llor Sánchez
Fecha actualización: mayo 2023

Avda Infante Juan Manuel 14
30011 Murcia

info.efiap@carm.es
http://efiapmurcia.carm.es/

ÍNDICE

RESUMEN

Este tema tiene por objeto el estudio de la normativa existente en materia de protección de datos, deteniéndonos en el estudio de la 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), para lo cual se hará una introducción, se determinará su marco normativo, se dará un concepto de Protección de datos y se delimitará su ámbito de aplicación. Además, se estudiarán los principios reguladores del RGPD y los derechos existentes en esta materia para los titulares de los datos. Por último, se verá cómo se tutelan esos datos de carácter personal.

OBJETIVOS

Conocer la normativa básica de protección de datos y, en especial, sus principios reguladores, así como los derechos de las personas con respecto a nuestros datos de carácter personal.

1. LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL. DISPOSICIONES GENERALES.

1.1. Introducción. Marco normativo.

A modo de introducción, podemos decir que vivimos en la sociedad de la información, teniendo lugar a diario el tratamiento de millones de datos personales. Así, facilitamos nuestros datos personales cuando abrimos una cuenta en el banco, cuando solicitamos participar en un concurso, cuando reservamos un vuelo o un hotel, cada vez que efectuamos un pago con la tarjeta de crédito o cuando navegamos por Internet.
El nombre y los apellidos, la fecha de nacimiento, la dirección postal o de correo electrónico, el número de teléfono, el DNI, la matrícula del coche y muchos otros datos que usamos a diario constituyen información valiosa que podría permitir identificar a una persona, ya sea directa o indirectamente.
Los ejemplos sobre cómo puede tratarse nuestra información en la sociedad digital y los resultados que ofrece son muy numerosos:

Algo tan simple como nuestra dirección de correo electrónico del trabajo suele indicar quiénes somos y en qué trabajamos y con ello una primera aproximación a nuestro perfil económico y nuestros intereses profesionales.

El derecho fundamental a la protección de datos es la capacidad que tiene el ciudadano para disponer y decidir sobre todas las informaciones que se refieran a él. Es un derecho reconocido en la Constitución Española y en el Derecho Europeo, que ha estado protegido en nuestro país hasta hace poco por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y actualmente se encuentra regulado por el Reglamento General de Protección de Datos, que entró en vigor el 25 de mayo de 2018, y que establece las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y las normas relativas a la libre circulación de tales datos.

Más en concreto, **la Constitución española** establece en su **artículo 18** lo siguiente:

> "*Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen*", añadiendo en su apartado 4 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*"

La protección de las personas con respecto al tratamiento automatizado de datos de carácter personal se desarrolló inicialmente por la Ley Orgánica 5/1992, de 29 de octubre. Con anterioridad a la aprobación de este texto legal España había firmado el 28 de enero de 1982 el Convenio comunitario sobre esta materia, aprobado y ratificado, para su entrada en vigor en el ámbito de nuestro país, el 1 de octubre de 1985.

La citada Ley Orgánica 5/92 fue derogada y sustituida por la Ley Orgánica de Protección de Datos de Carácter Personal, que adaptó nuestro Derecho interno a las orientaciones normativas de la Unión Europea y, en concreto, a la Directiva Comunitaria 1995/46, de 24 de octubre, del Parlamento Europeo y del Consejo, relativa a la protección de las personas físicas en el tratamiento de datos personales y a la libre circulación de estos datos. Asimismo, hemos de tener en cuenta que la Carta de los Derechos Fundamentales de la UE lo reconoce en el ámbito comunitario como un derecho fundamental (artículo 8).

El 25 de mayo de 2018 entró en vigor 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 –RGPD-). Los reglamentos son normas que tienen efecto directo lo que significa que se aplican directamente a los Estados miembros sin necesidad de que éstos adopten ninguna norma de trasposición al Derecho interno. Es por ello que la Comisión eligió esta vía con el fin de terminar con la dispersión normativa existente entre los países miembros. Así, con el RGPD tenemos una norma jurídica europea que conforma un Derecho único para toda la Unión al reemplazar a las leyes nacionales.

Por ello, en aras al principio de seguridad jurídica, existe la obligación de los Estados de eliminar situaciones de incertidumbre derivadas de la existencia de normas en el derecho nacional incompatibles con el europeo, lo que obliga a depurar el ordenamiento jurídico interno, y a derogar todo aquello que contradiga el RGPD.

La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales adaptó el derecho español al modelo establecido por el RGPD, introduciendo novedades mediante el desarrollo de materias contenidas en el mismo.

Junto a ello esta Ley Orgánica también incluyó los derechos digitales. Hoy identificamos con bastante claridad los riesgos y oportunidades que el mundo de las redes ofrece a la

ciudadanía, y corresponde a los poderes públicos impulsar políticas que hagan efectivos los derechos de la ciudadanía en Internet, por lo que el legislador abordó el reconocimiento de un sistema de garantía de los derechos digitales que encuentra su anclaje en el artículo 18.4 de la Constitución Española.

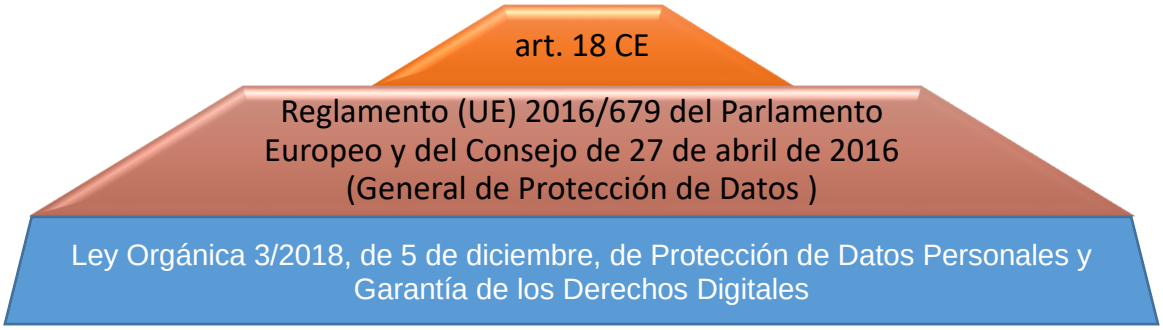
La norma trata de alinear el Ordenamiento con el RGPD abordando la materia con distintos objetivos:

a) Adaptar las previsiones generales del RGPD en el ámbito nacional con el límite del margen de apreciación que se concede a los Estados.

b) Regular sectores de actividad que requieren de un marco específico, ya sea por razón de la naturaleza de la actividad del tratamiento, ya sea por razón de los riesgos eventualmente asociados al tratamiento.

c) Integrar en nuestro Ordenamiento un marco de tutela de los derechos digitales, con fundamento en el mandato de desarrollo legal de garantías respecto del uso de la informática del artículo 18.4 de la Constitución Española.

Así pues, a modo de resumen, en nuestro Ordenamiento Jurídico, el marco normativo en esta materia se compone de las siguientes normas:



1.2. Delimitación conceptual.

El artículo 1 del RGPD señala como objeto la protección de derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales. También añade que la libre circulación de los datos personales en la Unión no podrá ser restringida ni prohibida por motivos relacionados con la protección de las personas físicas en lo que respecta al tratamiento de datos personales.

Partiendo de ese precepto, la primera cuestión a tratar será determinar qué hemos de entender por datos personales.

El artículo 4 del RGPD da un concepto de **datos personales**, definiéndolos como "*toda información sobre una persona física identificada o identificable (el interesado)".*

Ahora bien, es preciso, en segundo lugar, determinar frente a qué tiene lugar dicha protección.

El artículo 4 contiene una serie de definiciones, fundamentales para entender el significado de determinados términos empleados por el mismo a lo largo de su articulado.

Así, destacamos:

Fichero	Responsable del tratamiento o responsable	Encargado del tratamiento o encargado	Destinatario
• conjunto estructurado de datos de carácter personal • cualquiera que sea la forma o modalidad en que se crea, almacena, se organice y su acceso.	• persona física o jurídica, autoridad pública, servicio u otro organismo • solo o con otros • determina fines y medios del tratamiento.	• persona física o jurídica, autoridad pública, servicio o cualquier otro organismo • que trata datos personales por cuenta del responsable del tratamiento.	• persona física o jurídica, autoridad pública, servicio u otro organismo • al que le comunican datos personales • sea un tercero o no.

Junto a estas definiciones, el artículo 4 enumera muchas más, entre las que hay que destacar la "*seudonimización*", que se considera una medida de seguridad que consiste en la información que, sin incluir los datos denominativos de un sujeto afectado - es decir aquéllos que lo pueden identificar de manera directa -, sí que potencialmente permiten, a través de la asociación con información adicional, determinar quién es el individuo que está detrás de los datos seudonimizados, y la "*elaboración de perfiles*", que define como toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses,

fiabilidad, comportamiento, ubicación o movimientos de dicha persona física. En este sentido hay que destacar el derecho a no ser objeto de decisiones automatizadas íntimamente conectado a esta definición, lo cual ha cobrado mucha relevancia dado que cada vez son más numerosos los tratamientos basados en dicha elaboración, como la publicidad conductual basada en perfiles de navegación on line.

1.3. Ámbito de aplicación del RGPD.

El ámbito de aplicación de la Ley viene regulado en los artículos 2 y 3 del RGPD, que distingue entre ámbito de aplicación material y territorial.

a) Ámbito material.

El RGPD se aplica a todos los tratamientos total o parcialmente automatizados de datos y también a los tratamientos no automatizados de datos contenidos o destinados a ser incluidos en un fichero; en nuestros días los tratamientos que tienen un mayor impacto sobre los derechos de los ciudadanos son los realizados por medios automáticos, mientras que los totalmente manuales son relativamente raros.

Quedan **excluidos** de su ámbito de aplicación los siguientes tratamientos:

- En el ejercicio de una actividad no comprendida en el ámbito de aplicación del Derecho de la Unión. Un ejemplo de este tipo de tratamientos sería el de los tratamientos de datos relacionados con la seguridad nacional.
- Por parte de los Estados miembros, cuando lleven a cabo tratamientos relacionados con la Política Exterior y de Seguridad Común de la UE.
- Los efectuados por una persona física en el ejercicio de actividades exclusivamente personales o domésticas, es decir, en el marco de su vida personal y familiar y con fines que podrían describirse como particulares. Ejemplos de este tipo de tratamientos serían las agendas personales o el uso de algún servicio de almacenamiento de fotografías “on line”.
- 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 (La aplicación de esta excepción puede ser diferente según el Estado miembro que la aplique, ya que existe una Directiva sobre protección de datos en el ámbito policial y judicial penal -Directiva de Policía- con peculiaridades en los tratamientos de datos en prevención y persecución de delitos).

b) **Ámbito Territorial.**

Según su artículo 3.1, el RGPD será aplicable al tratamiento de datos personales en el contexto de las actividades de un establecimiento del responsable o del encargado en la Unión, independientemente de que el tratamiento tenga lugar en la Unión o no, es decir, es aplicable siempre que exista un establecimiento en la Unión, con independencia del país en que ese establecimiento esté localizado.

Por otro lado, la definición del RGPD incluye no sólo a los responsables, sino también a los encargados. El RGPD reconoce la evolución de la figura del encargado, que en la actualidad tiene una influencia mucho mayor en la forma en que se desarrollan los tratamientos, por lo que le atribuye expresamente determinadas obligaciones, previendo además que posibles incumplimientos, más allá de la responsabilidad que pueda sustanciarse ante el responsable en el marco de la relación contractual que les une, dan lugar también a responsabilidades administrativas.

El Reglamento establece su aplicabilidad al tratamiento de datos personales de interesados que residan en la Unión por parte de responsables o encargados que no estén situados en territorio de la Unión cuando realicen actividades de tratamiento relacionadas con:

- la oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si a estos se les requiere su pago, o
- el control de su comportamiento, en la medida en que este tenga lugar en la Unión.

Una previsión de este tipo es apropiada a las características de los tratamientos de datos en el mundo actual, el mundo de internet, donde las operaciones pueden realizarse a distancia y, en la práctica, muchos servicios de la sociedad de la información están organizados de tal manera que se prestan a todo el mundo desde la sede central de la compañía.

1.4. Del registro de ficheros al registro de actividades del tratamiento.

Con el RGPD desapareció la primera de las obligaciones a realizar por parte del responsable que trataba datos de carácter personal con la LOPD: la notificación de ficheros ante el Registro General de Protección de Datos.

Si bien esta inscripción de ficheros desapareció, el RGPD regula en su artículo 30 el denominado "**Registro de actividades de tratamiento"** de la siguiente forma:

"1. Cada responsable y, en su caso, su representante llevarán un registro de las actividades de tratamiento efectuadas bajo su responsabilidad. Dicho registro deberá contener toda la información indicada a continuación:

a. *el nombre y los datos de contacto del responsable y, en su caso, del corresponsable, del representante del responsable, y del delegado de protección de datos;*
b. *los fines del tratamiento;*
c. *una descripción de las categorías de interesados y de las categorías de datos personales;*
d. *las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales;*
e. *en su caso, las transferencias de datos personales a un tercer país o una organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49, apartado 1, párrafo segundo2, la documentación de garantías adecuadas;*
f. *cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos;*
g. *cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 32, apartado 13.*

2. Cada encargado y, en su caso, el representante del encargado, llevará un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta de un responsable que contenga:

a. *el nombre y los datos de contacto del encargado o encargados y de cada responsable por cuenta del cual actúe el encargado, y, en su caso, del representante del responsable o del encargado, y del delegado de protección de datos;*
b. *las categorías de tratamientos efectuados por cuenta de cada responsable;*
c. *en su caso, las transferencias de datos personales a un tercer país u organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en*

el artículo 49, apartado 1, párrafo segundo, la documentación de garantías adecuadas;

d. *cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 30, apartado 1.*

3. Los registros a que se refieren los apartados 1 y 2 constarán por escrito, inclusive en formato electrónico.

4. El responsable o el encargado del tratamiento y, en su caso, el representante del responsable o del encargado pondrán el registro a disposición de la autoridad de control que lo solicite.

5. Las obligaciones indicadas en los apartados 1 y 2 no se aplicarán a ninguna empresa ni organización que emplee a menos de 250 personas, a menos que el tratamiento que realice pueda entrañar un riesgo para los derechos y libertades de los interesados, no sea ocasional, o incluya categorías especiales de datos personales indicadas en el artículo 9, apartado 1, o datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10."

La existencia de los derogados Registros de Ficheros supuso una herramienta de ayuda y un punto de partida para la creación y gestión de los Registros de actividades de tratamiento. En el caso de las Administraciones públicas las obligaciones previas a la notificación de los referidos ficheros incluían un ejercicio severo de descripción exhaustiva y descripción de la legitimación que justificaba el tratamiento. Los tratamientos realizados por las Administraciones públicas se llevan a cabo mostrando su legitimidad de modo análogo, en cierta forma, a la publicación de la Disposición correspondiente, como dictaba la LOPD; además, se les da publicidad a través de la página Web de la Administración pública a la que corresponda para que el ciudadano pueda tener constancia de la base jurídica de los tratamientos a los que sus datos estén sometidos.

2. PRINCIPIOS RELATIVOS AL TRATAMIENTO (ART. 5 RGPD).

Los principios del tratamiento constituyen el fundamento del sistema europeo de protección de datos, tal y como se formulan, y son lo que le diferencia de otros modelos de protección de datos o privacidad.

En el RGPD cada principio tiene asignada una denominación propia que, en general, se corresponde con el modo en que se han identificado comúnmente en la doctrina, la jurisprudencia y la actuación de los operadores y de las autoridades de protección.

2.1. Principio de licitud, transparencia y lealtad.

Consiste en que los datos deben ser tratados de manera lícita, leal y transparente para el interesado. Este principio reconoce que el derecho a la protección de datos implica que los datos solo pueden ser tratados con el consentimiento del interesado o cuando la ley lo permita porque existan motivos que justifiquen que esa voluntad del interesado deba ceder ante otros derechos o intereses. Es el artículo 6.4 del RGPD el que establece las diferentes legitimaciones del tratamiento de los datos.

Por ejemplo, el tratamiento de datos puede resultar necesario para la ejecución de un contrato, o para que un organismo público pueda ejercer sus poderes o satisfacer un interés público.

Al mismo tiempo, este principio excluye que los datos sean tratados sin proporcionar la información necesaria al interesado para que entienda el objeto y fines del tratamiento, sus consecuencias y posibles riesgos, y pueda, en su caso, decidir sobre él. Este principio impide, por ejemplo, que la finalidad del tratamiento se exprese de forma vaga y confusa.

2.2. Principio de la "Limitación de la finalidad".

Este principio tiene dos partes:

- Por un lado, obliga a que los datos sean tratados con una o varias finalidades determinadas, explícitas y legítimas (relacionado íntimamente con el principio anterior). La finalidad del tratamiento ha de estar claramente definida, es decir, es posible que las finalidades sean descritas de un modo amplio, pero siempre que una descripción de ese tipo permita al interesado o a las autoridades de control conocer qué tipo de actividades se incluyen en ella. El hecho de que se exija que sean legítimas supone que todas están permitidas por el ordenamiento jurídico. En ese sentido, finalidades que resulten ilegales, como sería por ejemplo discriminar en el acceso a un puesto de trabajo a personas solteras, o casadas, o a personas de una determinada confesión religiosa, nunca pueden servir como base para el tratamiento de los datos.

- La segunda parte del principio es la que prohíbe que los datos recogidos con unos fines determinados, explícitos y legítimos sean tratados posteriormente de una manera incompatible con esos fines. El RGPD no impide tratar los datos de manera diferente a cuando se recogieron, lo que prohíbe es tratamientos para fines no compatibles. Menciona cuatro casos de finalidades que se consideran siempre compatibles: los de archivística en interés público, investigación científica e histórica y fines estadísticos.

2.3. Principio de "Minimización de datos".

No es posible, según este principio, recabar y tratar datos simplemente por si pudieran resultar útiles o "*por tenerlos*". Si para una finalidad concreta, el responsable no necesita tener determinados datos, no podrá recabarlos. Por ejemplo, si para una finalidad determinada no es necesario que el responsable conozca las pautas de navegación de un usuario, no podrá hacer ese seguimiento

2.4. Principio de exactitud.

Los datos deben ser exactos y, si fuera preciso, actualizados, debiendo adoptarse todas las medidas razonables para que se rectifiquen o supriman los datos inexactos en relación a los fines que se persiguen. Es importante tener en cuenta este principio, puesto que de muchos tratamientos de datos se derivan decisiones que pueden afectar a los derechos o intereses de los titulares de los datos.

Por ejemplo: que la compañía suministradora de electricidad o gas mantenga datos erróneos sobre sus clientes, podría dar lugar, desde no proporcionar el servicio que se ha contratado, hasta emitir facturas a los clientes equivocados.

2.5. Principio de "Limitación del plazo de conservación".

La conservación de los datos debe limitarse en el tiempo al logro de los fines que el tratamiento persigue. Una vez que esas finalidades se han alcanzado, los datos deben ser borrados o, al menos, desprovistos de todo elemento que permita identificar a los interesados.

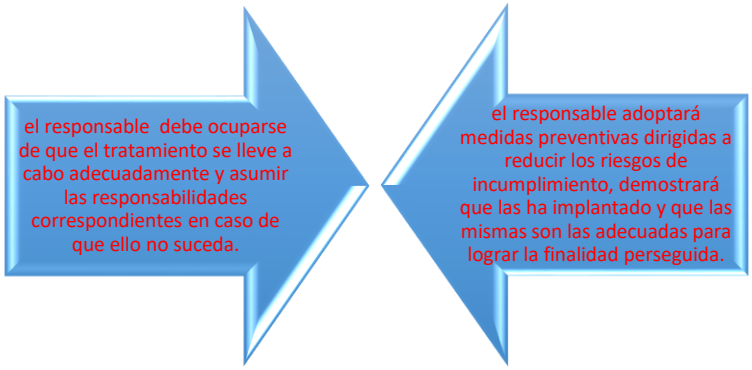
Hay casos en los que el RGPD sí permite casos de tratamientos ulteriores de los datos: con fines de archivística en interés público, investigación científica e histórica y fines estadísticos, para el cumplimiento de una obligación legal del responsable, o para que el responsable pueda ejercer acciones legales (art. 17.3 RGPD).

2.6. Principio de "Integridad y confidencialidad".

Impone a quienes tratan datos la obligación de actuar proactivamente con el objetivo de proteger los datos que manejan frente a cualquier riesgo que amenace su seguridad.

2.7. Responsabilidad proactiva.

Por último, aunque no se trate de un principio en sentido estricto, hay que hacer referencia a la **"***Responsabilidad proactiva***"** regulada en el art. 24 RGPD, que en síntesis, exige una actitud consciente, diligente y proactiva por parte de las organizaciones frente a todos los tratamientos de datos personales que lleven a cabo:



3. LA LEGITIMACIÓN PARA EL TRATAMIENTO DE DATOS PERSONALES.

El punto de partida para el tratamiento de datos personales es determinar la base jurídica que justifique o legitime las operaciones de dicho tratamiento y se encuentran recogidos en el Art. 6 RGPD. Al respecto señalar que las letras c) y e) son la base jurídica más habitual para el tratamiento de datos por parte de las Administraciones públicas.

a) **El consentimiento:** es la manifestación de voluntad libre por la que el afectado acepta el tratamiento mediante una declaración o una clara acción afirmativa, ya sea verbal o por escrito -por medios electrónicos o no-, marcando una casilla de un sitio web en internet, escogiendo parámetros técnicos para la utilización de servicios de la sociedad de la información, o con cualquier otra declaración o conducta que indique claramente en este contexto que el interesado acepta. El silencio **NO** se considera consentimiento, y en el caso de que haya varios fines habrá que consentir cada uno de ellos, aunque podrían agruparse si hubiera vinculación.

   En ningún caso hay aplicación retroactiva, dado que las normas del RGPD no se aplican a tratamientos anteriores al momento en que produce plenos efectos.

b) **La relación contractual:** el tratamiento es necesario para ejecutar un contrato en el que el interesado es parte, o para aplicar a petición de éste medidas precontractuales.

c) **El cumplimiento de una obligación legal aplicable al responsable del tratamiento o el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento:** Esta base jurídica del tratamiento de datos personales, contemplada en el artículo 6.1.c) y e) del RGPD, será como regla general la utilizada por parte de las Administraciones públicas.

   La finalidad del tratamiento para el *cumplimiento de una obligación legal* debe quedar determinada en la norma que la establezca. Y la finalidad del tratamiento para el *cumplimiento de una misión de interés público o para el ejercicio de poderes* debe ser necesaria para el cumplimiento o ejercicio de los mismos.

d) **El interés vital:** el tratamiento es necesario para proteger intereses vitales (=esencial para la vida) del interesado o de otra persona física. Esta base se puede calificar como subsidiaria ya que debe aplicarse cuando no pueda basarse el tratamiento en ninguna otra base jurídica (por ejemplo, el tratamiento en un control de epidemias o en situaciones de emergencia humanitaria).

e) **El interés legítimo**: En este supuesto no basta con la concurrencia de un interés legítimo sino que es necesario que éste prevalezca sobre los intereses, derechos o libertades fundamentales del interesado, es decir, exige que se lleve a cabo una ponderación, especialmente cualificada cuando el afectado sea un menor.

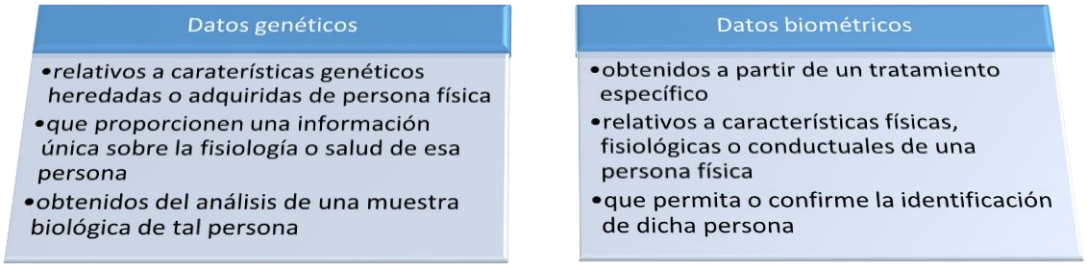
   Cuando la base jurídica sea ésta, se refuerzan las garantías para el tratamiento de los datos, por ejemplo en el deber de informar al interesado, ya que además de indicar el interés legítimo como base jurídica, deben especificarse los intereses legítimos concretos del responsable o del tercero que lo realicen, tanto si los datos se han obtenido del afectado como si no ha sido así. También se refuerza el derecho a oponerse por motivos relacionados con su situación personal.

Algún ejemplo de interés legítimo sería la prevención del fraude, el marketing directo o las trasmisiones de datos para garantizar la seguridad en redes.

4. TRATAMIENTO DE CATEGORÍAS ESPECIALES DE DATOS (DATOS ESPECIALMENTE PROTEGIDOS).

El RGPD, junto a los datos especialmente protegidos "*típicos*" como son las opiniones políticas, las convicciones religiosas o filosóficas, la afiliación sindical, los que revelen el

origen racial o étnico, y los relativos a la salud o a la vida u orientación sexual de una persona, incorpora nuevas categorías de datos como son los datos genéticos y los datos biométricos.



La regla general contemplada en el Reglamento es la prohibición del tratamiento de categorías especiales de datos, si bien recoge un amplio abanico de excepciones Art. 9 RGPD (consentimiento explícito del interesado, cumplimiento de obligaciones en el ámbito laboral o de seguridad social y protección de intereses vitales, entre otras)

Sobre los tratamientos realizados con las finalidades de tipo sanitario o social se prevé que el tratamiento se realice por un profesional sujeto a deber de secreto o bajo su responsabilidad, así como por cualquier otra persona sujeta a la obligación de secreto. Finalmente, se admite que los Estados miembros puedan mantener o introducir condiciones adicionales, incluidas limitaciones, sobre los tratamientos de datos genéticos, biométricos o de salud.

5. DERECHOS DE LAS PERSONAS.

Las principales obligaciones establecidas por la normativa de protección de datos recaen sobre el responsable del tratamiento, que deberá facilitar su cumplimiento y participar del mismo. Algunas de estas obligaciones disponen de una vertiente activa al generar su correspondiente acción de garantía y defensa, convirtiéndose en verdaderos derechos de los ciudadanos en relación con el tratamiento de su información de carácter personal. EL RGPD modifica el elenco de los derechos conocidos y reconocidos -en materia de protección de datos- por la normativa nacional y europea hasta su promulgación.

Asimismo, en cuanto a las *condiciones generales* para el ejercicio y atención de los derechos:

- se consolida la obligación de atender los derechos a menos que se acredite la imposibilidad de identificar al interesado;

- se establece el plazo de un mes prorrogable por dos más según la complejidad y número de solicitudes para la atención de su ejercicio;
- se plasma de manera definitiva la posible respuesta al ejercicio del derecho por medios electrónicos si el mismo se ejercitó por dichos medios, salvo que el interesado manifieste lo contrario;
- para el supuesto de que el responsable decida no dar curso a la solicitud del afectado, se consolida la obligación de informar en el plazo de un mes acerca de las razones de dicha negativa y sobre la posibilidad de acudir a la autoridad de control o a los órganos judiciales en caso de desacuerdo.

A su vez, se refuerza la "*gratuidad*" en el ejercicio de los derechos, salvo en el supuesto específico de solicitudes manifiestamente infundadas o excesivas, especialmente debido a su carácter repetitivo, en que será posible cobrar un canon razonable en función de los costes administrativos afrontados para facilitar la información o la comunicación, realizar la actuación solicitada, o, incluso, negarse a actuar respecto de la solicitud. También se faculta al responsable del tratamiento para solicitar información adicional que garantice suficientemente la identificación del afectado.

5.1. Derecho de información en la recogida de datos.

Las Administraciones públicas u Órganos administrativos -responsables del tratamiento- deberán facilitar a los interesados toda la información que precisen en relación con el tratamiento de sus datos personales. Una primera tarea en orden al cumplimiento de esta obligación de información consiste en la correcta cumplimentación por parte de los responsables de los tratamientos de los registros y/o fichas relativas a sus actividades de tratamiento.

Sin embargo, la más importante obligación de las Administraciones u Órganos responsables de los tratamientos en relación con los derechos en materia de protección de datos, es su deber de informar a todos los interesados -de manera expresa e inequívoca- de la existencia de dicho tratamiento de datos personales, de la identidad y dirección del responsable del tratamiento, de su finalidad, de los destinatarios, de la posible obligatoriedad de las respuestas y de la posibilidad de ejercer sus derechos.
El RGPD incrementa la información que habrá de facilitarse al interesado **cuando los datos se recaben de éste**, en relación a la normativa anterior. Son los artículos 12 "Transparencia de la información, comunicación y modalidades de ejercicio de los derechos del interesado" y 13 "Información que deberá facilitarse cuando los datos personales se obtengan del interesado" del RGPD, los que recogen ampliamente este

derecho; para facilitar el cumplimiento del mismo, la AEPD ha publicado la Guía para el cumplimiento del deber de informar en la que se especifica que, cuando los datos personales se recaben de los interesados, se puede facilitar la "*información por capas*", distinguiendo entre una información básica (primer nivel) y una información adicional (segundo nivel).

La justificación jurídico-práctica de la denominada "información por capas" se encuentra en la necesaria exigencia de claridad, concisión y fácil acceso a la información, y su objetivo es la comprensión, transparencia y adecuación al tipo de tratamiento de datos realizado por el responsable del tratamiento.

El RGPD se pone aún más exigente **cuando no se recaben los datos directamente del interesado**: deberá además informársele de las "Categorías de datos que se van a tratar", de la "Fuente de la que proceden los datos personales", y, en su caso, sobre si proceden de "Fuentes de acceso público". Asimismo, se clarifica el plazo aplicable para informar al interesado en este caso, siendo el mismo –con carácter general y "a más tardar"- de "un mes", o, en otro caso, debiendo producirse la información al interesado en el momento de la primera comunicación al interesado, si los datos se usan para ese fin, o de la primera cesión/comunicación de dichos datos a un tercero en el supuesto de que se pretenda la misma.

Ya refiriéndonos a ambos supuestos -tanto si los datos personales se han obtenido del interesado o no- las medidas a adoptar por el responsable del tratamiento para facilitar la información se pueden estructurar del siguiente modo:

- La información que se facilite ha de ser concisa, transparente, inteligible, accesible, fácil de entender y presentarse en un lenguaje claro y sencillo, en especial la dirigida específicamente a los niños.
- La información será facilitada por escrito u otros medios, incluso electrónicos, si procede.
- La información podrá facilitarse verbalmente, cuando lo solicite el interesado.

Por último hay que señalar que el RGPD establece excepciones específicas al deber de información, recogidas en sus artículos 13.4 y 14.5, distinguiendo si se han recabado del interesado o no.

¡OJO! Consecuencia práctica de lo anterior ha sido que todas las cláusulas, cupones, fichas, cuestionarios o formularios (incluyendo los utilizados en las páginas web), de empresas y Administraciones públicas han tenido que adaptarse a los requisitos a los que se ha hecho mención, comprendiendo en todo caso información concisa, transparente, inteligible, clara y sencilla en relación con el tratamiento de los datos que pretenda realizar el responsable.

5.2. El ejercicio de los derechos del interesado.

Como titular de sus datos de carácter personal, el interesado por el tratamiento puede ejercitar ante el responsable, Administración u Órgano administrativo que esté tratando dichos datos personales, sus derechos de acceso, de rectificación, de supresión -incluida su variante de derecho al olvido-, de portabilidad, de oposición, y de limitación del tratamiento.

En el plano protector y reactivo que corresponde a las autoridades de control, la letra a) del apartado 1 del artículo 58 del RGPD confiere una serie de poderes a las Autoridades de Control de Protección de Datos cuando los responsables, o en su caso, encargados, no cumplen con estos derechos.

Los referidos derechos se regulan específicamente en los **artículos 15 a 22 del RGPD**:

- **Derecho de acceso:** los interesados por los tratamientos pueden conocer si sus datos de carácter personal están siendo tratados por parte de la Administración pública o del Órgano administrativo responsable del tratamiento, qué datos son objeto de dicho tratamiento, la finalidad del mismo, el origen de los citados datos y si se han comunicado o se van a comunicar a un tercero. Una vez ejercitado, el responsable debe responder, y, en caso de estimar el acceso, debe elegir la forma por la cual ofrecerá la información, garantizando la obtención por el interesado de una copia de sus datos y de la información asociada al mismo (artículo 15).

¡OJO! no confundir este derecho con el de acceso a la información pública de la Ley de Transparencia ni con el derecho de acceso en un procedimiento administrativo.

Una vez ejercitado el derecho de acceso, *la Administración u Órgano responsable debe responder*, y, en caso de estimar dicho acceso, elegir la forma por la cual ofrecerá la información, garantizando la obtención por el interesado de una copia de sus datos y de la información asociada a los mismos. Se podrá considerar repetitivo el ejercicio del

derecho de acceso en más de una ocasión durante el plazo de seis meses, a menos que exista causa legítima.

Los *medios más habituales para facilitar el acceso* son la visualización en pantalla, la remisión de escrito, copia o fotocopia remitida por correo -certificado o no-, la obtención de telecopia, la remisión de correo electrónico u otro sistema de comunicación electrónica y, en fin, la puesta a disposición por el responsable al interesado de cualquier otro sistema adecuado para el acceso. El RGPD se inclina a favor de la ***gratuidad*** del primer acceso mediante copia de la información, posibilitando la exigencia de un canon orientado a sufragar los costes de las ulteriores solicitudes.

- **Derecho de rectificación:** Supone la posibilidad de que mediante su ejercicio el titular de los datos, sin dilación indebida, obtenga la modificación de aquellos que sean inexactos o incompletos, debiendo en la solicitud de rectificación indicar qué datos desea que se modifiquen o corrijan, y acompañar la documentación justificativa en la que base su pretensión (artículo 16).

Así, 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.

- **Derecho de supresión - "Derecho al olvido":** El derecho de supresión tiene por objeto la eliminación, sin dilación indebida, de los datos personales cuando concurra alguno de los supuestos a los que se hará mención. 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. El RGPD contempla algunas excepciones que justifican la improcedencia en la atención del mismo, por ejemplo, cuando deba prevalecer la libertad de expresión y/o de información (artículo 17).

Junto a la supresión, en el mismo artículo, el RGPD regula el "Derecho al olvido", es decir, ejercer el derecho de supresión y de oposición a los buscadores de internet para impedir la difusión de la información cuando ésta es obsoleta o no tiene relevancia ni interés público (también en lo que se refiere a fotos y vídeos).

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 la 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"

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 Española de Protección de Datos.

- **Derecho a la limitación del tratamiento:** el RGPD recoge que cuando se den alguna de las condiciones que regula en su artículo 18, el interesado tendrá derecho a obtener del responsable una limitación en el tratamiento de sus datos.
- **Derecho de portabilidad de los datos:** este derecho supone que los interesados por los tratamientos puedan solicitar la recuperación de los datos personales que estén siendo tratados de forma automatizada por un determinado responsable a fin de trasladarlos a otro responsable de su elección. Esto será posible cuando el tratamiento se base en el consentimiento o en la relación contractual y se efectúe por medios automatizados (artículo 18).

En consecuencia, el derecho a la portabilidad de los datos (artículo 20) implica el derecho a recibir los datos personales facilitados en un formato estructurado, de uso común y lectura mecánica, y poder transmitirlos a otro responsable del tratamiento, sin que lo impida el responsable al que se los hubiera facilitado, siempre que sea técnicamente posible.

- **Derecho de oposición y decisiones individualizadas:** La mayor parte de los tratamientos de datos requiere el consentimiento del titular salvo que concurran las excepciones previstas en la normativa aplicable.

El derecho de oposición puede ejercerse en cualquier momento, por motivos relacionados con la situación particular del interesado, debiendo cesar el tratamiento de los datos realizado por el responsable, salvo que se acredite un interés legítimo o sea necesario para el ejercicio o defensa de reclamaciones. Asimismo, puede ejercerse cuando el tratamiento tenga por objeto la mercadotecnia directa (artículo 21).

En los supuestos en que el tratamiento se base en "el cumplimiento de una misión de interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento" o cuando sea necesario para satisfacer intereses legítimos perseguidos por el responsable o un tercero (siempre que no prevalezcan derechos o libertades fundamentales del interesado), el responsable del tratamiento 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 para la formulación, el ejercicio o la defensa de reclamaciones.

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 personales que le conciernan, incluida la elaboración de perfiles en la medida en que esté relacionada con la citada mercadotecnia.

Por otra parte el artículo 22 recoge que todo interesado tiene **derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado** de su información de carácter personal, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar.

Las **excepciones** a este derecho se concretan en los supuestos en que dicho tratamiento sea necesario para la celebración o ejecución de un contrato, esté permitido por el Derecho de la UE o de los Estados miembros, o bien exista consentimiento explícito del titular de los datos.

En estos casos, la Administración pública responsable del tratamiento debe adoptar las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado y, 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 basado únicamente en un tratamiento automatizado de los datos personales: 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.

5.3. Limitaciones en el ejercicio de los derechos.

En el RGPD se establecen una serie de limitaciones del ejercicio de los derechos de los interesados; es su artículo 23 el que ofrece un catálogo de los supuestos que justifican las limitaciones del ejercicio de derechos.

La existencia de estas limitaciones requiere su formulación por Ley, que ha de respetar los derechos y libertades fundamentales. Asimismo, se exige que se trate de una medida necesaria y proporcionada en una sociedad democrática para el logro de los objetivos, fijándose expresamente el contenido mínimo de dicha disposición para asegurar el establecimiento de las garantías adecuadas.

6. TUTELA DE LOS DATOS: LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS Y EL DELEGADO DE PROTECCIÓN DE DATOS.

6.1. La Agencia Española De Protección De Datos.

El artículo 51 del Reglamento General de Protección de Datos (RGPD) estipula que cada Estado miembro establecerá que una o varias autoridades públicas independientes (denominadas autoridades de control) supervisen su aplicación con el fin de proteger los derechos y las libertades fundamentales de las personas físicas en lo que respecta al tratamiento y de facilitar la libre circulación de datos personales en la UE. Asimismo, su artículo 54 impuso a los Estados miembro la adopción de un régimen jurídico específico que se debía establecer mediante y respecto de todos los elementos que recoge el referido artículo 54.

La autoridad encargada de velar por el cumplimiento de la legislación en materia de protección de datos en España es la **Agencia Española de Protección de Datos**,

La LOPDGD regula el régimen de la AEPD, calificándola de autoridad administrativa independiente de ámbito estatal, de las previstas en el artículo 109 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público. Aunque mantiene un cierto grado de relación con el Ministerio de Justicia se acerca al modelo de comisionado parlamentario incorporando en el camino una nueva denominación para su dirección, la Presidencia, y la figura de un Adjunto. Para el nombramiento de ambos, allí donde antes no hubo requisitos ahora se exigirá una reconocida competencia profesional, en particular en materia de protección de datos, que implicará una convocatoria pública y la previa evaluación del mérito, capacidad, competencia e idoneidad de los candidatos antes de ser propuestos al Parlamento acompañada de un informe justificativo. Las candidaturas serán ratificadas en 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. Por otra

parte, se integran en el Consejo de profesionales de la privacidad, la seguridad o la transparencia.

Actualmente el Estatuto de la AEPD se regula en el Real Decreto 389/2021, de 1 de junio, atendiendo a la necesidad de adecuar la estructura orgánica de la AEPD al RGPD y la LOPDGD, y contribuye a dotar de mayor seguridad jurídica a la organización y funcionamiento de la Agencia, al adecuarla a las nuevas competencias establecidas en dichas normas, cumpliendo asimismo el principio de transparencia, eficiencia ya que entre otras cuestiones, no impone cargas administrativas adicionales.

Un aspecto capital de la AEPD es el de su **independencia,** por lo que el RGPD estipula en su artículo 52 que el miembro o los miembros de cada autoridad de control serán ajenos en el desempeño de sus funciones y en el ejercicio de sus poderes a toda influencia externa, ya sea directa o indirecta, y no solicitarán ni admitirán ninguna excepción. Se abstendrán de cualquier acción incompatible con sus funciones, ni participarán en actividad profesional, remunerada o no, que resulte incompatible. En este sentido se pronuncia el artículo 4 del RD 389/2021 al señalar que "*Ni el personal ni los miembros de los órganos de la Agencia Española de Protección de Datos podrán aceptar ni solicitar instrucciones de ninguna entidad pública o privada*."

Con la finalidad de supervisar la aplicación del RGPD, éste atribuye a las autoridades de control, y por tanto a la AEPD, un elenco de **funciones y de potestades** en sus artículos 57 y 58, respectivamente, que conforman sus competencias, y que vienen recogidas en nuestro ámbito nacional en el artículo 5 del RD 389/2021. Entre sus poderes están los de investigación, poderes correctivos y poderes de autorización y consultivos.

El RGPD estipula 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 RGPD. Entre las funciones que atribuye a las autoridades de control está la de tramitar las reclamaciones presentadas por un interesado o por un organismo 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.

El Reglamento de desarrollo de la LOPD, aprobado por el Real Decreto 1720/2007, de 21 de diciembre (RLOPD), establece los procedimientos para la tramitación de las reclamaciones, ya se trate de tutelas de derecho o de procedimientos relativos al ejercicio de la potestad sancionadora. Las reclamaciones por tutela de derechos se han de formular por los propios interesados o por quien debidamente los represente y se han de resolver en un plazo máximo de seis meses por el procedimiento establecido en el RLOPD. En el supuesto de reclamaciones que dieran lugar a un procedimiento sancionador se pueden realizar actuaciones previas encaminadas a determinar la concurrencia de motivos que lo justifiquen, que no podrán extenderse más de 12 meses. Iniciado el procedimiento sancionador tendrá una duración máxima de 6 meses.

En todo caso, **se inadmitirán 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 vulneración de los derechos reconocidos.

Los plazos para la tramitación de los procedimientos, que no podrán superar los 18 meses, quedarán automáticamente suspendidos cuando deba recabarse información, consulta o pronunciamiento de un órgano de la UE o de una Autoridad de control, conforme establece el RGPD, hasta la notificación del pronunciamiento a la AEPD.

Las resoluciones que pongan fin a los procedimientos de reclamación serán objeto de publicación.

Establece el RGPD que toda persona física o jurídica tendrá derecho a la tutela judicial efectiva contra una decisión de una autoridad de control jurídicamente vinculante que le concierna, por lo que las resoluciones de la AEPD agotan la vía administrativa, pudiendo 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.

6.2. El Delegado de Protección de Datos.

El RGPD configura una serie de "*medidas de responsabilidad activa*" aplicables a los responsables y, en ocasiones, a los encargados del tratamiento de datos, medidas que puede distinguirse en: análisis de riesgos, registro de actividades de tratamiento, medidas de seguridad, protección de datos desde el diseño, y por defecto, notificación de "violaciones de seguridad de los datos", evaluación de impacto sobre la protección de datos y finalmente, el delegado de protección de datos.

Una medida de responsabilidad activa, es la figura del *Delegado de protección de datos* regulado en los artículos 37-39 del RGPD que establece una serie de supuestos de designación obligatoria por parte de los responsables y encargados, siempre que:

- El tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial.
- Las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala, o
- Las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos personales con arreglo al artículo 9 y de datos relativos a condenas e infracciones penales a que se refiere el artículo 10.

La obligación de que las "**autoridades u organismos públicos**" designen un delegado de protección de datos (DPD) se enmarca en la finalidad de la norma de reforzar la seguridad jurídica y práctica para las personas físicas, los operadores económicos y las autoridades públicas en el tratamiento de datos de carácter personal. La rápida evolución tecnológica y la globalización han planteado nuevos retos para la protección de los datos personales. La tecnología permite que las autoridades públicas utilicen datos personales en una escala sin precedentes a la hora de realizar sus actividades; ello ha transformado tanto la economía como la vida social, y ha de facilitarse aún más la libre circulación de datos personales dentro de la Unión, garantizando al mismo tiempo un elevado nivel de protección de los datos personales, particularmente en aquellas entidades que llevan a cabo operaciones de tratamiento de datos a gran escala, algo que realizan habitualmente las Administraciones públicas y sus entidades del sector público.

No regula el Reglamento la titulación específica para el DPD, pero sí exige unas características muy concretas para que pueda ser desarrollado, que son:

- Conocimientos especializados en Derecho.
- Práctica en materia de protección de datos.
- Capacidad para desarrollar las funciones del artículo 39, que básicamente consisten en información y asesoramiento al responsable o al encargado del tratamiento y a los empleados que se ocupan del mismo, supervisión de la

normativa, cooperación con la autoridad de control, y asesoramiento sobre la evaluación de impacto en la materia.

A ello hay que añadir, dentro del sector público, que debe tener conocimientos sólidos de las normas y los procedimientos administrativos de la organización.
El RGPD prevé que el Delegado podrá desarrollar su actividad a tiempo completo o parcial y también que podrá formar parte de la plantilla del responsable o del encargado del tratamiento o desempeñar sus funciones en el marco de un contrato de servicios.

Además, debe tenerse en cuenta que el Delegado actúa como asesor y supervisor interno, por lo que ese puesto no puede ser ocupado por personas que, a la vez, tengan tareas que impliquen decisiones sobre la existencia de tratamientos de datos o sobre el modo en que van a ser tratados los datos (p.ej.: responsables de ITC, o responsables de seguridad de la información).

Señala el RGPD que cabe que el DPD "*forme parte de la plantilla del responsable o del encargado del tratamiento o desempeñar sus funciones en el marco de un contrato de servicios*"

Ahora bien, de las recomendaciones de la AEPD se desprende que, para el caso de la Administración Públicas, es muy cuestionable que se acuda a personal externo, a la vista de sus funciones dentro de los organismos, del perfil jurídico que se le requiere y de la incardinación dentro de la estructura administrativa.

La nota más importante en este aspecto es la **independencia funcional** que debe tener el DPD según recoge el RGPD, de forma que no recibirá ninguna instrucción en el desempeño de sus funciones, ni podrá ser destituido ni sancionado por el ejercicio de las mismas. En contrapartida, el DPD está sometido al deber de secreto o confidencialidad. Por tanto, es necesario que el diseño organizativo por el que se opte garantice plenamente esta independencia.

Lo expuesto conlleva la necesidad de que ese puesto de trabajo, o unidad orgánica que se cree al efecto, no pueda estar incorporado en la línea jerárquica de ninguna estructura, pero a su vez, debe estar adscrita a un departamento o área de actuación. La AEPD considera que debe adscribirse a órganos o unidades de naturaleza

"horizontal" pero, por encima de todo, lo que exige es que se salvaguarde la independencia en su funcionamiento. Esta exigencia reafirma el hecho de que no quepa en la Administraciones públicas un DPD externo mediante contrato de servicios, cuya independencia podría quedar en entredicho.

Las **funciones del Delegado de Protección de Datos**, que serán de información, asesoramiento y supervisión, se encuentran especificadas en el artículo 39 del RGPD, y que según el documento de la AEPD "*El Delegado de Protección de Datos en las Administraciones Públicas*", las mismas se pueden concretar en las siguientes áreas:

- ✓ Respecto al cumplimiento.
- ✓ Respecto a la relación con los interesados.
- ✓ Respecto a la seguridad.
- ✓ Respecto a la prevención.
- ✓ Respecto a la cooperación.
- ✓ Respecto a la formación.

En la CARM, el Consejo de Gobierno, mediante Acuerdo de 1 de agosto de 2018, ha nombrado a la Inspección General de Servicios Delegado de Protección de Datos de la Administración General de la Comunidad Autónoma de la Región de Murcia, sus Organismos y Entidades públicas empresariales, Sociedades Mercantiles Regionales, Fundaciones, Consorcios y otras entidades de derecho público. (EXCLUIDOS: la Consejería de Familia e Igualdad de Oportunidades y el Instituto Murciano de Acción Social, los Centros Docentes de la Consejería de Educación, Juventud y Deportes y el Servicio Murciano de Salud que tendrán su propio DPD).

El correo electrónico de contacto del Delegado de Protección de Datos es: dpdigs@listas.carm.es de manera que el responsable o el encargado del tratamiento debe contar con la ayuda de este Delegado de Protección de Datos y dirigirse a dicho correo en cualquier momento para dudas o auxilio en esta materia.

Por otra parte resulta extensa la referencia al Delegado de Protección de Datos en la LOPDGD cuya figura se implanta en un número significativo de sectores. Los órganos y organismos del Sector Público tienen obligación de designar un Delegado de Protección de Datos que cuente con la debida cualificación, de garantizarle los medios necesarios para el ejercicio de sus funciones y de notificar la designación a la AEPD para su inclusión en el Registro público de Delegados de Protección de Datos.

El Delegado de Protección de Datos no tiene responsabilidad a título personal por las posibles infracciones en materia de protección de datos cometidas por su organización, por el mero hecho de serlo. 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.

Por último señala que el Delegado 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 AEPD en el plazo máximo de un mes.

7. LA LEY ORGANICA 3/2018, DE 5 DE DICIEMBRE, DE PROTECCIÓN DE DATOS PERSONALES Y GARANTÍA DE LOS DERECHOS DIGITALES.

La LOPDGDD debe ser leída e interpretada siempre en el marco del RGPD. Ello exige a sus intérpretes, y en particular a los llamados delegados de protección de datos, aproximarse a esta materia con un enfoque global e integrador.

Veamos ahora a modo de resumen, algunos de los aspectos más importantes de la LOPDGDD, no recogidos en el tema, pero que no dejan de ser fundamentales en esta materia:

- En relación con las disposiciones generales, se reconoce específicamente el derecho de acceso y, en su caso, de rectificación o supresión por parte de quienes tuvieran vinculación con personas fallecidas por razones familiares o de hecho y a sus herederos. La medida limita el ejercicio de estos derechos cuando el fallecido lo hubiera prohibido.
- La LOPDGDD concede una importancia fundamental a la protección de los menores. La Ley fija en 14 años la edad a partir de la cual se puede prestar consentimiento de manera autónoma, sujeta el tratamiento de este tipo de datos al desarrollo de una evaluación de impacto en la protección de datos y requiere disponer de un delegado de protección de datos a los centros docentes, y a las federaciones deportivas. Por último, la afectación a los derechos de los menores será un elemento a considerar en la determinación y graduación de las sanciones.
    - En sede de derechos digitales, regula expresamente el derecho a solicitar la supresión de los datos facilitados a redes sociales u otros servicios de

la sociedad de la información por el propio menor o por terceros durante su minoría de edad, se recoge el derecho a la educación digital, que implicará una revolución en los planes de estudio y en la formación del profesorado, y se contempla por primera vez la responsabilidad de padres, madres y centros escolares por el tratamiento de información de menores en internet, estableciendo el deber de la Administración de diseñar políticas públicas de concienciación digital. Estas medidas se conciben como una aproximación provisional emplazando al Gobierno a impulsar en el plazo de un año desde la entrada en vigor de la ley orgánica, un proyecto de ley dirigido específicamente a garantizar los derechos de los menores ante el impacto de Internet.

- El derecho Español adapta, en el Título dedicado a los derechos de las personas, el principio de transparencia. Se regula el modo en que debe informarse a las personas acerca del tratamiento de sus datos optándose, específicamente en el ámbito de internet, por un sistema de información por capas que permita al ciudadano conocer de forma clara y sencilla los aspectos más importantes del tratamiento, pudiendo acceder a los restantes a través de un enlace directos. Por otra parte, los operadores deberán discernir cuándo se ejercen derechos propiamente digitales como la rectificación en internet, la actualización de informaciones en medios de comunicación digitales o el derecho al olvido en búsquedas de Internet, incluidas redes sociales, y servicios equivalentes (se exceptúa la supresión cuando los datos hubieran sido facilitados por terceros en el ejercicio de actividades personales o domésticas.)
- El Título IV incorpora disposiciones que regulan tratamientos sectoriales. Particularmente destacable resulta su alto impacto en las relaciones laborales. Aquí, además de la definitiva consolidación legislativa de la posición histórica de la Agencia Española de Protección de Datos (AEPD) sobre sistemas de denuncias internas, debe prestarse particular atención a los controles laborales. Así, por un lado, la Ley actualiza las garantías del derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo. Asimismo, refuerza las garantías del derecho a la intimidad en relación con el uso de dispositivos digitales puestos a disposición de los empleados, complementando la regulación del derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral, de los que deberán ser informados. Y por otro, la Agencia ha propuesto que se recogieran

en la Ley los sistemas de denuncias internas anónimas, a través de los cuales puede ponerse en conocimiento de una entidad privada la comisión de actos o conductas que pudieran resultar contrarios a la normativa. Estos sistemas son imprescindibles para que las personas jurídicas puedan acreditar la diligencia necesaria para quedar exentas de responsabilidad penal. De este modo, la Ley dota a las empresas de un mecanismo que les permite conciliar su propio derecho con el derecho a la protección de datos de las personas.

- El legislador en el Título V ha decidido reforzar el marco de obligaciones del responsable y del encargado del tratamiento. En lo que se refiere al encargado la LOPDGDD recupera principios del Real Decreto 1720/2007 y los armoniza con los de RGPD. Cabe destacar la importancia central que adquiere el papel de ciertos encargados en la notificación de violaciones de seguridad. Una de las cuestiones a las que debe prestarse una atención significativa será sin duda a la extensión de los criterios que obligan a desarrollar una evaluación de impacto relativa a la protección de datos, en casos como tratamientos a gran escala, cuando se produzca un tratamiento masivo que implique a un gran número de afectados o conlleve la recogida de una gran cantidad de datos personales, o en supuestos interpretables como el de los grupos de afectados en situación de especial vulnerabilidad.
- En materia sancionadora la LOPDGDD, refuerza el marco procedimental y aterriza en nuestro Derecho el régimen del RGPD confiriendo particular importancia a la intervención del delegado de protección de datos y de los sistemas de resolución extrajudicial de conflictos. La LOPDGDD describe un catálogo de conductas típicas con la triple diferenciación propia de las infracciones y sanciones administrativas en nuestro Ordenamiento jurídico, que las distingue entre muy graves, graves y leves, pero tomando en consideración la diferenciación que el RGPD establece al fijar la cuantía de las sanciones. La categorización de las infracciones y de las sanciones se introduce, por lo tanto, a los solos efectos de determinar los plazos de prescripción de unas y otras, teniendo la descripción de las conductas típicas como único objeto la enumeración de manera ejemplificativa de algunos de los actos sancionables que deben entenderse incluidos dentro de los tipos generales establecidos en la norma europea.
- Se regulan por primera vez los derechos digitales de los españoles. La LOPDGDD recoge novedades significativas en esta materia. El Título X posee un contenido complejo que aúna diversas estrategias. En primer lugar, se ordena

una relectura de nuestro sistema de derechos fundamentales que deberá ser interpretado de modo funcional al mundo digital. Se apuesta por una internet segura e inclusiva, con garantía de acceso universal y se fomentan las políticas públicas. El legislador confiere particular importancia a los derechos de los menores y a su educación, a los derechos de los trabajadores, considerando el derecho a la desconexión de la vida laboral. Asimismo, aborda aspectos nucleares de la vida digital como el impacto de los medios de comunicación y los buscadores, modulando los derechos de rectificación, olvido y portabilidad, y ordena los efectos del fallecimiento en el mundo digital.

EL SECTOR PÚBLICO Y LA LOPGDD.

Por último hay que destacar que el sector público debe prestar una particular atención a la nueva LOPDGDD. El ámbito de materias que, bien habilitan para la acción pública legitimando un tratamiento, bien impone deberes adicionales, es particularmente voluminoso.

Cabe destacar por su significativo impacto:

a) Los órganos y organismos del Sector Público quedan obligados a publicar en su página web el inventario de las actividades de tratamiento de datos personales que realizan, identificando quién trata los datos, con qué finalidad y qué base jurídica legitima ese tratamiento, así como a incluir en su página web información clara y precisa destinada a los administrados sobre el ejercicio de los derechos de acceso, rectificación, supresión, derecho a la limitación del tratamiento, así como a la portabilidad y oposición.
b) Mayor transparencia de las sanciones impuestas al Sector Público.
   Las infracciones cometidas por los órganos y organismos del Sector Público 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 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. Cuando 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.

c) Nueva regulación de la aportación de documentación por parte de los administrados: modificación del artículo 28 de la Ley 39/2015.

   Ya la ley 30/1992 reconocía a los administrados el derecho a no aportar a los procedimientos administrativos los documentos que obrasen en poder de la Administración, o que hubiesen sido elaborados por ésta. La base jurídica del tratamiento de los datos personales por la Administración era el consentimiento del administrado, que se entendía tácitamente concedido si el interesado no se oponía expresamente

   Tanto el RGPD como la nueva Ley Orgánica eliminan la necesidad de recabar el consentimiento, ni siquiera tácito, del administrado, al establecer como base jurídica legitimadora principal del tratamiento de datos personales por órganos y organismos del Sector Público el cumplimiento de una misión en interés público o, particularmente, el ejercicio de poderes públicos

   Asimismo, la nueva redacción otorgada por la Ley Orgánica al artículo 28 de la Ley 39/2015 reconoce al administrado la posibilidad de oponerse a que órganos y organismos del Sector Público consulten o recaben los citados documentos, pero en ese caso el administrado deberá aportarlos necesariamente para que la Administración pueda conocer que concurren en él los requisitos establecidos por la norma. En caso contrario no podrán estimar su solicitud, precisamente porque no habría demostrado los requisitos requeridos

   En todo caso dicho derecho de oposición no juega en los casos de potestades de verificación o inspección.

   Por último, podemos añadir en este sentido que los órganos y organismos del Sector Público pueden verificar, sin necesidad de solicitar consentimiento del interesado, la exactitud de los datos personales manifestados por los administrados que obren en poder de los órganos y organismos del Sector Público.

d) Notificación de actos administrativos: identificación de los administrados. La nueva Ley Orgánica impide el uso conjunto de apellidos, nombre y número completo del documento de identificación oficial de las personas en aquellos actos administrativos que vayan a ser objeto de notificación y/o publicación.

   A partir de la entrada en vigor de la Ley Orgánica:

- en las notificaciones se identificará a la persona mediante su nombre y apellidos, añadiendo cuatro cifras numéricas aleatorias de su documento identificativo oficial,
- en las publicaciones de anuncios se identificará a la persona exclusivamente con el número de su documento identificativo, o, en el caso de no disponer del mismo, sólo mediante su nombre y apellidos.

En su relación con los sujetos privados, los órganos y organismos del Sector Público pueden comunicar los datos personales de los administrados a sujetos de derecho privado que lo soliciten:

i. bien cuando cuenten con el consentimiento de los administrados,
ii. bien, cuando aprecien que concurre en el sujeto privado solicitante un interés legítimo que prevalezca sobre los derechos e intereses de los administrados concernidos.

e) Registros de personal del sector público: legitimación del tratamiento. La nueva Ley Orgánica establece que la base legitimadora del tratamiento de datos personales que realizan los registros de personal del sector público es el ejercicio de potestades públicas. Estos registros pueden tratar los datos personales que sean estrictamente necesarios para el cumplimiento de sus fines relativos a infracciones y condenas penales e infracciones y sanciones administrativas.

f) Tratamiento de datos personales en investigación sanitaria. La LOPDGDD flexibiliza el tratamiento de datos para la investigación en salud:

• amplía las finalidades para las que se puede otorgar el consentimiento al tratamiento,

• recoge la posibilidad de reutilizar la información sobre la que se ya se haya prestado consentimiento con anterioridad,

• recoge el uso de datos pseudonimizados como una opción para facilitar la investigación sanitaria incluyendo garantías para evitar la reidentificación de los afectados y

• regula las garantías de este tratamiento, incluyendo la intervención de los Comités de Ética de la Investigación o, en su defecto, del Delegado de Protección de Datos o de un experto en protección de datos personales.

BIBLIOGRAFÍA.

LEGISLACIÓN EUROPEA

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 (General de Protección de Datos).

LEGISLACIÓN ESTATAL

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales.