Universidad Miguel Hernández de Elche

Facultad de Ciencias Sociales y Jurídicas de Elche

GRADO EN DERECHO

Trabajo Fin de Grado

Curso Académico 2019-2020

UNIVERSITAS
Miguel Hernández

TRABAJO DE FIN DE GRADO

"PROTECCIÓN DE DATOS PERSONALES ¿CÓMO Y CUÁNDO EJERCITAR NUESTROS DERECHOS? CUESTIONES PRÁCTICAS"

ALUMNA: VERÓNICA LÓPEZ RODRÍGUEZ

TUTOR: PROF.DR. ALFONSO ORTEGA GIMÉNEZ

*Cuando George Orwell escribió la obra "**1984**", propuso quizá,un inventario de problemas a los que se iban a enfrentar las libertades y el ciudadano como sujeto de esas libertades. En dicho inventario, creo que ocupan un carácter especialmente importante los riesgos que entrañan las nuevas tecnologías para la intimidad de la persona y las consecuencias nocivas para la libertad que potencialmente suponen.*

RESUMEN:

Es clara la especial incidencia que el uso de las Nuevas tecnologías de la información (TIC) han tenido en nuestra sociedad, cambiando sustancialmente nuestra manera de relacionarnos, conectando la sociedad a nivel global y sobre todo reflejando la patente la capacidad de extensión que la información alcanza. Se hace impensable que dicha manera de relacionarnos, la aparición de un nuevo mundo el ciber-mundo, que conecta a nivel mundial a todos los ciudadanos, no impactara en nosotros generando conflictos que originarían el surgimiento de nuevos derechos y motivarían la configuración de nuevas formas y niveles de protección de dicha información, en concreto la protección de datos personales.

El presente trabajo, pretende realizar un recorrido de esa evolución jurídica, haciendo especial incidencia en el régimen jurídico español y europeo de la protección de datos personales, desde su origen hasta la actual normativa. Se abordará los diferentes ámbitos de aplicación de la ley: ámbito objetivo, subjetivo y territorial; desgranaremos uno a uno los derechos de los que la regulación actual nos dota y establecer los cauces procedimentales para ejercitar estos derechos.

Se intentará reflexionar sobre la situación actual de aquellos derechos que recoge la LOPDGDD que todavía no se han desarrollado y de los cuales la AEPD no tiene en todos una competencia directa[1], de palabras de la directora de la AEPD , Mar España(2018): *"de (…) Agencia es competente únicamente en los regulados en los artículos 89 a 94, es decir somos competentes de la garantía de 6 de los 17 reconocidos ",* esto ocasiona cierta incertidumbre acerca de la competencia o regulación de los derechos digitales restantes, Mar apunta (2018) *"(…)* , salvo en el ámbito de los derechos de los menores en Internet y el derecho a la educación digital, para los que sí se establece la competencia de las Administraciones educativas y la del Gobierno para remitir un proyecto de Ley, en todos los demás, la Ley no atribuye la competencia; se puede deducir de los Reales Decretos de estructura de los ministerios*".*

La configuración a su vez de nuevos derechos como el de "testamento digital" junto con el conocido derecho al olvido, derecho a la desconexión laboral, el acceso universal a internet son novedades significativas en la actual normativa.

Este trabajo es fruto de la compilación de normativas, informes, guías públicas y pretende propiciar una visión más práctica de estos derechos a los ciudadanos para que finalmente puedan hacer un uso efectivo y seguro de sus datos[2].

[1] Entrevista a Mar España directora de la AEPD, extracto de la Obra "Especial nueva Ley Orgánica de protección de datos y garantía de los derechos digitales", Wolter Kluwer 11 de diciembre de 2018.

[2] Vid. En el mismo sentido este artículo hace especial referencia que aunque la protección de datos preocupa a los ciudadanos, muy pocos leen las políticas de privacidad

Según un artículo del periódico digital público que hacía alusión a un estudio del CIS[3] de mayo de 2018, "*5% de los internautas españoles lee "algunas veces", "raramente" o "nunca" las políticas de privacidad de las páginas web que visita"* significativamente **sin embargo "la *protección de los datos personales preocupa "mucho" o "bastante" a tres de cada cuatro encuestados (un 76,1%)*",** es decir, el uso que hagan de nuestro datos preocupa pero desgraciadamente casi **nadie se lee las instrucciones**.

La agencia en este caso ha comenzado una campaña información pedagógica realizando "Guías para los ciudadanos"[4]

En cada uno de ellos estudiaremos los procedimientos para poder ejercer los derechos de forma correcta: las condiciones que se requieren, los formularios que se deben presentar, y los distintos medios existentes para ejercitarlos.

Por otro lado, aparece otra incógnita, **el grado de preparación de las empresas y de AAPP españolas para implantar la nueva LOPDGDD, parece que NO es mucho mejor que la de los ciudadanos de a pie**, como destaca en la entrevista la presidenta de la AEPD [5]*" hay tres millones de empresas que operan en nuestro país, incluyendo los autónomos y los profesionales" pero solo "número de Delegados de Protección de Datos designados hasta ahora es de unos 22.000"*, es por esto que la Agencia ha puesto en marcha el programa FACILITA[6], sin embargo las pequeñas y medianas empresas (PYMES) aunque cumplen con los requisitos que la legislación exige, solo un 39% han previsto o atendido solicitudes de ejercicio de los derechos de las personas[7].

Aparece a su vez una figura anteriormente desconocida, el Delegado de Protección de Datos, analizaremos a su vez también que trabajo tiene esta figura y su importancia en la implantación de las nuevas políticas de protección de datos.

---

https://www.publico.es/sociedad/proteccion-datos-cis-confirma-sospechamos-nadie-lee-politicas-privacidad.html, revisado 21/11/19

[3] Fuente CIS, Barómetro de mayo de 2018 http://datos.cis.es/pdf/Es3213mar_A.pdf

[4] https://www.aepd.es/media/guias/guia-ciudadano.pdf Guía práctica de la AEPD

[5] Extracto entrevista a la presidenta AEPD Mar España, incluida en la obra "Especial Ley Orgánica de Protección de datos y derechos digitales" Wolters Kluwer diciembre 2018 https://www.smarteca.es/my-reader/SMT2018025_00000000_0?fileName=content%2FEX0000140123_20181210.HTML&location=pi-493&publicationDetailsItem=SystematicI

[6] ProgramaFACILITA,consulta15/04/2019 https://www.servicios.agpd.es/AGPD/view/form/MDAwMDAwMDAwMDAwMDIxNzcxMjkxNTU1Mjg2NTYzMDI3?updated=true

[7] Estudio sobre protección de datos de la AEPD, abril y mayo de 2018, consulta el 15/04/2019 https://www.aepd.es/media/estudios/estudio-proteccion-de-datos-aepd-cepyme.pdf

Palabras clave. Delegado de Protección de Datos, Derechos Digitales, Protección de Datos, Consentimiento.

Summary

It is clear the special impact that the use of New Information Technologies (ICT) has had in our society, substantially changing the way we interact, connecting society at a global level and especially reflecting the patent the extension capacity that information achieves. It is unthinkable that this way of relating, the emergence of a new world, the cyber-world, which connects all citizens worldwide, will not impact us generating conflicts that would cause the emergence of new rights and motivate the configuration of new forms and levels of protection of such information, specifically the protection of personal data. The present work, tries to realize a route of that legal evolution, making special incidence in the Spanish and European legal regime of the protection of personal data, from its origin to the current regulation. The different areas of law enforcement will be addressed: objective, subjective and territorial scope; We will recount one by one the rights that the current regulation gives us and establish the procedural channels to exercise these rights.

Keywords. Delegate for Data Protection, Digital Rights, Data Protection, Consent.

ABREVIATURAS

- LOPDGDD: Ley Orgánica 3/2018, de 5 de diciembre de protección de datos y de garantía de derechos digitales.
- AEPD: Agencia Española de Protección de Datos.
- DPO: DELEGADO DE PROTECCIÓN DE DATOS
- RGPD: Reglamento general de protección de datos 2016/679 del Parlamento Europeo y del Consejo.
- NT: Nuevas tecnologías.
- TIC: Tecnologías de la información y comunicación
- PYMES: Pequeñas y medianas empresas.

I. INTRODUCCIÓN:

En nuestro día a día, se hace necesario el uso continuado de datos personales, sea simplemente para la contratación, compra o adquisición de servicios o para la utilización de aparentemente inofensivas aplicaciones móviles.

Coincidencia o no, comienzo este trabajo el 12 de marzo de 2019 el buscador de Google de mi ordenador, me recuerda que es el 30 aniversario de internet; esa idea visionaria de Tim Berners-Lee, el cual aprovechó el protocolo de las tres "w" y lo desarrolló para el uso y expansión de Internet (Word Wide Web).

Sin embargo, esa creación no está exenta de controversia, incluso años después su creador ha visto necesario que se aplique un código de buenas prácticas en el uso de internet. El uso desmedido de nuestros datos por las principales redes sociales ha hecho que el creador de internet cree una nueva plataforma "Solid" cuyo sentido es el control de nuestros datos y ser una alternativa a las principales redes sociales"[8]

No hay que olvidar, que el nacimiento del derecho de protección de datos está íntimamente ligado a la aparición de la informática, las nuevas tecnologías de la información y cómo la manera de conectar y de trasladar información ha evolucionado de tal manera que nuestro concepto de intimidad entra en conflicto con el normal desarrollo de nuestra actividad social cotidiana.

Al igual que el Sr. Berners Lee, el ámbito jurídico ha visto necesaria la creación de códigos de conducta y el desarrollo de la regulación en materia de protección de datos, *"las normas surgen como consecuencia de una necesidad social, utilizando el derecho como fórmula de solución de conflictos*" (Delgado, 2010)[9]

Es en la nueva ley orgánica de protección de datos y derechos digitales de 3/2018 de 5 de diciembre de 2018 y el RGPD 2016/679, dónde se da respuesta a esta pregunta.

---

[8] El creador de la 'World Wide Web' crea una nueva red que da a los usuarios control sobre sus datos https://www.lavanguardia.com/tecnologia/20181001/452114001384/creador-internet-crea-red-usuarios-control-datos. Ese artículo se desprende de este otro artículo original https://www.fastcompany.com/90243936/exclusive-tim-berners-lee-tells-us-his-radical-new-plan-to-upend-the-world-wide-web (fecha consulta 12 marzo 2019)

[9] Delgado, Lucrecio Rebollo, y María Mercedes Serrano Pérez. "*Introducción a la protección de datos"*. Editorial Dykinson, s.l.i, 2010, pag.25

La LOPDGDD 3/2018 de 5 de diciembre se desarrolla como ley orgánica pues se trata de un derecho fundamentalmente protegido en nuestra norma magna en su art. 18.4 *"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".*

Ya el tribunal constitucional señaló en su Sentencia 94/1998, de 4 de mayo[10], el *"derecho a la protección de datos y se garantiza el control sobre sus datos, cualesquiera de datos personales y sobre su uso y destino".*

Por otro lado en la sentencia de 292/2000, de 30 de noviembre este derecho se *"* considera un derecho autónomo e independiente*, que* 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… permite a su vez saber quién…y para qué posee esos datos personales," dotando a esa persona de la capacidad de "oposición a esa posesión o uso".

El origen de este derecho que viene ligado al derecho constitucionalmente reconocido el derecho a la intimidad (art.18 CE), en conexión con su aptado 18.4 " 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", sin embargo este derecho se ha ido desligando y desarrollando como derecho autónomo como dice (Rebollo Delgado, 2008)[11]:

*"*Ésta es la circunstancia dada en lo relativo a la protección de datos , que sin abandonar la fundamentación originaria, ha evolucionado de forma muy significativa, incluso podriamos decir que adquiere autonomia, se independiza del derecho originario*"*

En palabras del Profesor Galán Muñoz[12]:

"(…)la tradicional definición del derecho a la intimidad, como derecho de corte exclusivamente negativo, se ha visto ya claramente superada por las posibilidades que nos ofrecen las modernas tecnologías de la información, tanto para captar, como para procesar o difundir datos que nos afectan muy directamente, lo que parece nos obligará a tener que replantearnos la tradicional conceptualización de dicho derecho fundamental o incluso a cambiarlo por uno más nuevo, amplio y adaptado a la nueva realidad de nuestra sociedad, como sería el denominado derecho a la privacidad*".*

[10] http://hj.tribunalconstitucional.es/HJ/eu-ES/Resolucion/Show/SENTENCIA/1998/94

[11] Delgado, Lucrecio Rebollo. *Vida privada y protección de datos en la Unión Europea*. Dykinson, Madrid, 2008, pag. 102.

[12]Muñoz, Alfonso Galán. *La protección jurídica de la intimidad y de los datos de carácter personal frente a las nuevas tecnologías de la información y comunicación*. Tirant lo Blanch, 2014.

Podemos afirmar por tanto que los conceptos D. Honor, Intimidad, Imagen y protección de datos están tan vinculados que en ocasiones se nos hace casi imposible su disección. Eso se desprende de que todos responden a un objetivo común la **protección constitucional a la vida personal y familiar**.

Sería por tanto quizás realizar una diferenciación con carácter previo de cada uno de los conceptos en base a la STC 292/2000[13]:

- Derecho a la propia imagen: "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"

✓ Diferencia. El concepto de dato personal abarca mucho más que la propia imagen, puede ser nombre y apellidos, una huella dactilar o incluso un dirección *IP.*

- Derecho a la intimidad: "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 éstos 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 jurídicosobre lapublicidad de lainformaciónrelativa al círculo reservado de su persona yfamilia, que se desea mantener al abrigo del conocimiento público. Lo que el artículo 18.1 de la Constitución garantiza, es, pues, el secreto sobre nuestra propia esfera de vida personal y, por tanto, veda que sean los terceros, particulares opoderes públicos, quienes decidan cuales son los contornos de nuestra vida privada".

✓ Podríamos decir que el derecho a la intimidad responde a una una esfera o ámbito de protección más reservada, se refiere a aquellas

[13] *https://forma2.inap.es/c4x/AEPD/AEPD19-01/asset/Webminar_1.pdf, curso sobre protección de datos de la AEPD para empleados de la administración local, del epígrafe "Desligando algunos derechos", exposición. Eduard Chaveli Donet*

actividades que se desarrollan en ese espacio más personal de nuestra vida.

- ✓ La protección de datos responderá a una protección de acuerdo con el carácter más sensible o menos sensible de estos, sin llegar a esa esfera tan intima, pero quizás,si en ocasiones casi solapándose.

- Derecho al honor. Aquí la diferenciación sea más fácil ya que el derecho al honor es un derecho reconocido no solo a las personas físicas sino también a las jurídicas, sentencias como la STC 9 de octubre de 1997 dispone:

*"*Las personas jurídicas también son titulares del derecho al honor, en la vertiente de buen nombre comercial de la empresa o de prestigio de la misma, que suponen una proyección pública del buen nombre y consideración ajenas, con trascendencia en el mercado. Las personas jurídicas pueden ser titulares, así, de un reconocimiento que los demás hacen de su dignidad, seriedad, probidad, solvencia, etc., por lo que también son susceptibles de sufrir un ataque o infracción de su honor o prestigio.Así, como se exponía en Sentencia"

- ✓ La protección de datos solo y exclusivamente protege a las personas físicas.

- El derecho de 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"
  - ✓ Es por tanto la proteccion de datos consiste en un poder de disposición y de control sobre los datos que faculta a la persona a decidir cuáles son los datos que se va a tratar o recabar por un tercero y su uso.
  - ✓ Suponen estas diferencias no solo en cuanto a su definición sino también en cuanto a su tratamiento procesal. Estableciendo para la protección de datos un procedimiento administrativo frente a la protección jurisdiccional de los otros como por ejemplo el derecho al hornor LO 1/82[14].

[14] https://www.boe.es/buscar/doc.php?id=BOE-A-1982-11196, ley para la protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen.

II. CONCEPTOS PREVIOS

Es necesario aclarar ciertos términos que serán utilizados para que su interpretación y aplicación sea uniforme, estas definiciones las extraemos del RGPD 2016/679.

a) Dato de Carácter personal:

Toda información sobre una persona física viva identificada o identificable; se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

Los datos personales que hayan sido anonimizados, cifrados o presentados con un seudónimo, pero que puedan utilizarse para volver a identificar a una persona, siguen siendo datos personales y se inscriben en el ámbito de aplicación del RGPD.

Los datos personales que hayan sido anonimizados**,** de forma que la persona no sea identificable e o deje de serlo, dejarán de considerarse datos personales[15]. Para que los datos se consideren verdaderamente anónimos, la este proceso debe ser irreversible.

El RGPD protege los datos personales independientemente de las técnicas o tecnologías utilizadas para su tratamiento, es tecnológicamente neutro y se aplica tanto para tratamientos automatizados como manual, siempre que se utilice un criterio predeterminado; tampoco importa su modo de conservación y en todos los casos, los datos están sujetos a los requisitos de protección establecidos en el RGPD.[16]

Ejemplos de datos personales:[17]

- nombre y apellidos
- domicilio,
- dirección de correo electrónico, del tipo nombre.apellido@empresa.com,
- número de documento nacional de identidad,
- de localización (como la función de los datos de localización de un teléfono móvil) (*),

[15] Vid. En el mismo sentido este artículo cuando se trata de estudios o estadísticas y siempre que los datos estén aninimizados de manera tal que sea imposible su reconocimiento a posteriori https://www.lavanguardia.com/vida/20191029/471274125624/ine-seguira-movimientos-moviles-estudio.html el INE seguirá movimientos móviles, para estudiar mejor en infraestructuras, 2019 Noviembre.

[16] (https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_es)

[17] (https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_es)

- dirección de protocolo de internet (IP),
- el identificador de una *cookie* (*),
- el identificador de la publicidad del teléfono
- los datos en poder de un hospital o médico, que podrían ser un símbolo que identificara de forma única a una persona.

(*) Cabe señalar que, en algunos casos, existe una legislación sectorial específica que regula, por ejemplo, el uso de los datos de localización o el uso de las «cookies»: la Directiva sobre intimidad y comunicaciones electrónicas (Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002 (DO L 201 de 31.7.2002, p. 37) y el Reglamento (CE) n.º 2006/2004 del Parlamento Europeo y del Consejo, de 27 de octubre de 2004 (DO L 364 de *9.12.2004, p. 1)*[18]

Ejemplos de datos NO considerados datos personales:

- número de registro mercantil

- dirección de correo electrónico, del tipo info@empresa.com

- datos anonimizados o con seudonimización: «seudonimización»: el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable

- Datos de fallecidos: El RGPD establece que solo serán objeto de protección los datos de las personas vivas. Pero establece que los estados miembros podrán regulas sobre el tratamiento de datos personales de estos y esto precisamente es lo que hace nuestra LOPDGDD en su Derecho relativo al Testamento Digital art.96.

[18] El 01/10/2019 en sentencia el TJUE (ECLI:EU:C:2019:801) ASUNTO C-673/17, decisión planteada por el Bundesgerichsthof (Alemania)el Tribuna Supremo de lo Civil y Penal, Alemania sobre el uso de COOKIES. En dicha sentencia declara que el consentimiento que el usuario de un sitio de internet debe dar para la colocación de cookies en su equipo o terminal y la consulta de éstas no es válida con la mera marcación por defecto de una casilla y retirarla si no desea su consentimiento. El tribunal subraya que el consentimiento debe ser específico, de modo que el hecho de que un usuario active el botón de en la participación en el juego organizado con fines promocionales no basta para considerar que éste se ha dado de manera su consentimiento para la colocación de cookies. Además, según el Tribunal de justicia, la información que le proveedor de servicios debe facilitar al usuario incluye tiempo durante el cual las cookies estarán activas y la posibilidad de que terceros tengan acceso a ellas. Extracto de noticias jurídicas http://noticias.juridics.com/actualidad/jurisprudencia/1445-la-colocacion-de-cookies-requiere-el-consentimiento-activo-de-los-internautas/

- Placas de matrícula de vehículos[19](existe ciertas aclaraciones al respecto, pues hay informes en una y otra dirección)

- El art.14 RGPD establece que la regulación de protección de datos personales no es aplicable a personas jurídicas. No obstante, cabe realizar una aclaración al respecto, dentro del ejercicio de la actividad normal de la persona jurídica, habrá una persona física que será el contacto de esa persona jurídica, **¿qué pasa con los datos de esa persona física, sus tratamientos de datos están incluidos o no?**

  La respuesta es Sí, los datos de esa persona física están dentro de los protegidos por la normativa en cuanto a protección de datos, pero, ese tratamiento de datos estará permitido siempre y cuando sea necesario en la relación con la empresa jurídica. El art. 14 RGPD establece que se entenderá amparado en el interés legítimo de ese tratamiento siempre que cumplan unos requisitos:

  i. Que los datos que se traten sobre esa persona sean necesario para la localización de la persona jurídica
  ii. Que la finalidad sea únicamente mantener esa relación con la persona jurídica.

b) Tipología de datos personales. ¿Son todos iguales?

También existen las categorías especiales de datos: en los que además de los datos de salud se encuentran los que puedan revelar tu origen étnico o racial, opiniones políticas, convicciones religiosas o fisiológicas, o afiliación sindical, así como el tratamiento de tus datos genéticos, biométricos (si te identificasen de manera unívoca), así como los relativos a tu vida sexual u orientación sexual. Nuevamente acudiremos al art 4 del RGPD para definir algún que otro concepto como:

- 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"*

[19] https://www.samuelparra.com/wp-content/uploads/2010/08/archivo_denuncia-matricula.pdf Procedimiento E/01173/2009 del 1 de Julio de 2009 en el que se aclara que "la comunicación mediante la colocación de la denuncia en el parabrisas del vehículo de la denunciante (refiriéndose a la persona que interpuso la denuncia en la AEPD), se ha de señalar que el citado boletín no refleja dato personal alguno de la denunciante, en la medida en la que los datos incluidos en el no permite su identificación"
Por otro lado respecto a la licitud del tratamiento sin consentimiento, el informe señala " (…) en principio, sólo se puede llevar a cabo (…) con el consentimiento del titular" sin embargo señala que existen determinados casos en el que los datos de un particular no requieran de la autorización previa exigida como regla general" poniendo como ejemplo " dichos datos de carácter personal se recojan para el ejercicio de las funciones propias de la Administración públicas, cuestión tal que se observa en el presente caso" fecha consulta 15/04/2019

El RGPD y nuestra LOPDGDD establece una norma general de **prohibición** del tratamiento de datos de categorías especiales de datos personales. Art 9.

Sin embargo, hay excepciones y estas excepciones a su vez sufren variaciones en cuanto contemplamos la normativa española y su desarrollo (véase notas al pie) estos casos son:

a) el interesado dio su consentimiento explícito para el tratamiento de dichos datos personales con uno o más de los fines especificados, excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición mencionada en el apartado 1 no puede ser levantada por el interesado;[20]

b) el tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social, en la medida en que así lo autorice el Derecho de la Unión de los Estados miembros o un convenio colectivo con arreglo al Derecho de los Estados miembros que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado;

c) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento (por ejemplo: Asistencia sanitaria urgente, comunicación de personas desaparecidas, accidentes de tráfico)

d) el tratamiento es efectuado, en el ámbito de sus actividades legítimas y con las debidas garantías, por una fundación, una asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que el tratamiento se refiera exclusivamente a los miembros actuales o antiguos de tales organismos o a personas que mantengan contactos regulares con

[20] Este precepto está establecido según el RGPD art.9.2, pero la LOPDGDD especifica en su artículo 9.1 lo siguiente : A los efectos del artículo 9.2.a) del Reglamento (UE) 2016/679, a fin de evitar situaciones discriminatorias, el solo consentimiento del afectado no bastará para levantar la prohibición del tratamiento de datos cuya finalidad principal sea identificar su ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico.

ellos en relación con sus fines y siempre que los datos personales no se comuniquen fuera de ellos sin el consentimiento de los interesados;

e) el tratamiento se refiere a datos personales que el interesado ha hecho manifiestamente públicos;

f) el tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial;(aquí incluiríamos a abogados y procuradores)

g) el tratamiento es necesario por razones de un interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales interesado (este artículo fue el que utilizaron para incluir el recientemente declarado inconstitucional art.58 bis de la 5/85 LOREG, introducido por la disposición final 3 de la LOPDGDD)[21]

h) el tratamiento es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social, sobre la base del Derecho de la Unión o de los Estados miembros o en virtud de un contrato con un profesional sanitario y sin perjuicio de las condiciones y garantías contempladas en el apartado 3[22];

i) 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,

[21] https://www.boe.es/boe/dias/2019/06/25/pdfs/BOE-A-2019-9548.pdf LEY ORGÁNICA DE PROTECCIÓN DE DATOS Y GARANTIAS DE DERECHOS DIGITALES.

[22] Los tratamientos de datos contemplados en las letras g), h) e i) del artículo 9.2 del Reglamento (UE) 2016/679 fundados en el Derecho español deberán estar amparados en una norma con rango de ley, que podrá establecer requisitos adicionales relativos a su seguridad y confidencialidad.

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

3. Los datos personales a que se refiere el apartado 1 podrán tratarse a los fines citados en el apartado 2, letra h),cuando su tratamiento sea realizado por un profesional sujeto a la obligación de secreto profesional, o bajo su responsabilidad, de acuerdo con el Derecho de la Unión o de los Estados miembros o con las normas establecidas por los organismos nacionales competentes, o por cualquier otra persona sujeta también a la obligación de secreto de acuerdo con el Derecho de la Unión o de los Estados miembros o de las normas establecidas por los organismos nacionales competentes.

Respecto a este grupo, es necesario destacar el tratamiento de datos personales relativos a condenas e infracciones, estos solo pueden llevarse a cabo bajo el control y la supervisión de las autoridades públicas.

c) Sujetos Obligados

El artículo 4.7 del Reglamento (UE) 2016/679 de 27 de abril de 2016, se define al responsable del tratamiento o **responsable como**:

- **Responsable** "la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros determine los fines y medios del tratamiento"

Esta persona puede ser tanto física como jurídica o una Administración pública que determina tanto la finalidad como los medios que se utilicen para el tratamiento de los datos personales de los interesados.

Aparece también otra definición, publicada por el Grupo de Trabajo del Artículo 29 (GT29) en su relevante dictamen 1/2010 sobre los conceptos de Responsable de tratamiento y encargado de tratamiento, básicamente establece que "cualquier persona física o jurídica, en los términos indicados, que decida sobre el tratamiento de los datos personales será considerada responsable de tratamiento", el responsable " debe asumir la responsabilidad del cumplimiento de las normas sobre protección de datos y de qué manera pueden los interesados ejercer sus derechos"

- **El encargado** es la persona encargada de tratar esos datos personales sin que pueda decidir sobre el tratamiento, el encargado es una persona o personas designada por el responsable de tratamiento de datos.

Además, esta figura además es determinante en cuanto la aplicación o no del RGPD, determinando la aplicación territorial, ya que según establece el art. 3.1 RGPD independientemente de dónde se realice el tratamiento, se deberá atender a dónde está el responsable del tratamiento de datos, porque ello va a determinar si es aplicable el RGPD incluso cuando el responsable recurre a un encargado fuera del territorio de la Unión Europea[23].

Además, este responsable de tratamiento está sometido al principio de responsabilidad, "tiene que adoptar las medidas técnicas y organizativas adecuadas para cumplir y demostrar el cumplimiento de la normativa aplicable sobre protección de datos personales" responsabilidad proactiva.

Además, deberá contemplar "la naturaleza, ámbito, en contexto y los fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de Las personas físicas" apartado 1 artículo 24 RGPD

En el art. 28 obligaciones del responsable del tratamiento de la ley orgánica 3/2018 de 5 de diciembre, "deberá tener en cuenta los mayores riesgos para los derechos y libertades fundamentales de los interesados, conforme al listado que se incluye en ese artículo" además de que deberá atender en todo momento al riesgo que implique el tratamiento de datos personales para el interesado[24]. Esto implica que no solo la responsabilidad se realiza en cuanto a ese tratamiento sino también la vigilancia de cómo se realiza ese tratamiento, sus consecuencias y riesgos.

- **Destinatario**: la persona física o jurídica, autoridad pública, servicio u otro organismo al que se comuniquen datos personales, se trate o no de un tercero. No obstante, no se considerarán destinatarios las autoridades públicas que puedan recibir datos personales en el marco de una investigación concreta en el marco de una investigación de conformidad con el derecho de la Unión o de los estados miembros; el tratamiento de tales datos por dichas autoridades públicas será conforme con las normas en materia de protección de datos aplicables a los fines del tratamiento".

- **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".

[23] http://curia.europa.eu/juris/liste.jsf?language=es&num=C-131/12, Sentencia SSTJ GoogleSpain y Google Inc contra AEPD, ámbito Territorial y Material 13 Mayo 2014.

[24]https://guiasjuridicas.wolterskluwer.es/Content/Documento.aspx?params=H4sIAAAAAAAEAMtMSbF1jTAAAkNjE0NDE7Wy1KLizPw8WyMDQwsDU0MzkEBmWqVLfnJIZUGqbVpiTnEqAIF-Erw1AAAAWKE

d) Agencia Española de Protección de Datos

La configuración del derecho a la protección de datos como un derecho autónomo y claramente diferenciado de los demás, hace necesaria la creación de una autoridad independiente que vele por el ejercicio de este derecho, dicha consideración está recogida en el Convenio 108 del Consejo de Europa (1981), fuente originaria internacional sobre la materia y se configura en la Directiva 95/43/CE, relativa a la protección de datos personales y la libre circulación de esos datos.

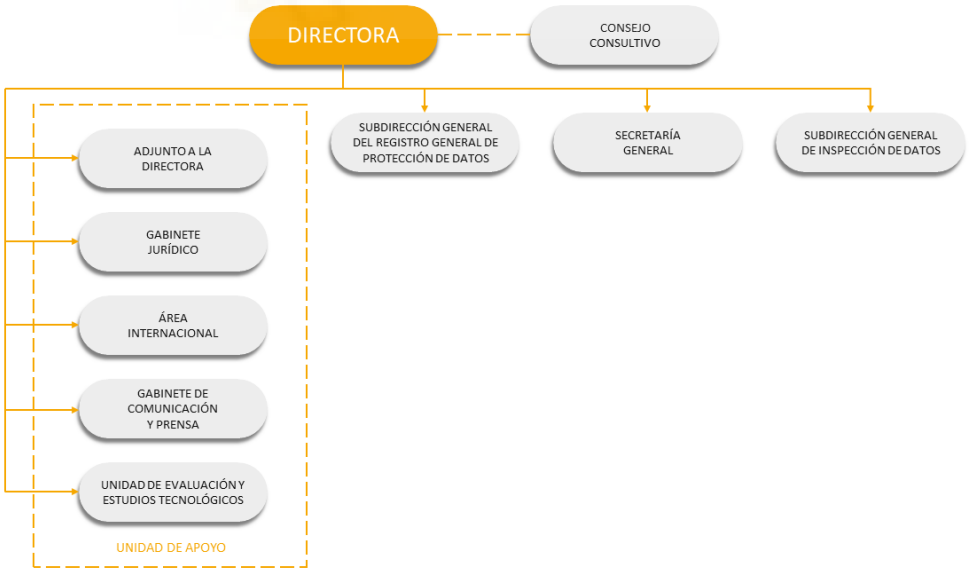
"*La creación de una autoridad de control que ejerza sus funciones con plena independencia en cada uno de los Estados miembros constituye un elemento esencial de la protección de las personas en lo que respecta al tratamiento de datos personales» (Considerando 62 de la Directiva 95/46)".*

El artículo 28.1 de la Directiva prevé que «estas autoridades ejercerán las funciones que le son atribuidas con total independencia».

En España se adoptó el criterio organizativo y funcional propuesto en el Convenio 108 y que luego pasaría a ser un rasgo esencial del modelo europeo: la atribución de la función de velar por el cumplimiento de la normativa de protección de datos a una autoridad independiente.

La Agencia Española de Protección de Datos goza de esa naturaleza de ente independiente, con presupuesto propio y plena autonomía funcional.

La AEPD se creó en 1992 y comenzó a funcionar en 1994.



Fuente: www. Aepd.es

Haremos referencia a la figura del director/a de la AEPD:

- DIRECTOR/A: Actualmente. Dña. Mar España Martí

La directora ostenta la representación de la Agencia y sus actos se consideran como actos propios de la Agencia[25].Es nombrada de ente los miembros del Consejo Consultivo y a propuesta del ministro de justicia. Tiene consideración de alto cargo con rango de Subsecretario. Es elegida por un tiempo de 4 años.

Los motivos de cese son: por fin de mandato, renuncia, fallecimiento o separación acordada por el Gobierno, estos pueden ser incumplimiento grave de sus obligaciones, incapacidad sobrevenida, incompatibilidad o condena por delito doloso.

Sus resoluciones ponen fin a la vía administrativa y son recurribles ante la Sala de lo Contencioso de la Audiencia Nacional.

La directora tiene un carácter independiente y ejercerá sus funciones con *"*dedicación exclusiva, plena independencia y total objetividad*".*

Sus funciones son entre otras:

- Autorizar las transferencias internacionales
- Iniciar, impulsar la instrucción y resolver los expedientes sancionadores.
- Instar la incoación de expedientes en el caso de infracciones[26]
- Autorizar la entrada en los locales en los que hallen los ficheros
- Además, representará a la Agencia en el ámbito internacional: en el Comité Europeo de Protección de Datos, ejerce la Secretaría permanente de la Red Iberoamericana de Protección de Datos.
- Además, realizará funciones de gestión como: adjudicar y formalizar contratos, aprobar gastos y ordenar pagos, programar la gestión de la Agencia

La directora es asistida en el ejercicio de sus funciones por una Unidad de Apoyo.

La Agencia Española de Protección de Datos ha designado como DPO a D. Manuel Villaseca López.

[25] Consultada la página de la AEPD, fecha de consulta 15/04/2019 https://www.aepd.es/agencia/transparencia/organigrama/direccion.html

[26] https://www.boe.es/boe/dias/2018/12/06/pdfs/BOE-A-2018-16673.pdf LOPDGDD.Regulados en los artículos 71,72,73 y 74 LOPDGDD y en el RGPD 83.5, 83.4,83.6, las sanciones prescriben: a) Las sanciones por importe igual o inferior a 40.000 euros, prescriben en el plazo de un año. b) Las sanciones por importe comprendido entre 40.001 y 300.000 euros prescriben a los dos años. c) Las sanciones por un importe superior a 300.000 euros prescriben a los tres años. 2. El plazo de prescripción de las sanciones comenzará a contarse desde el día siguiente a aquel en que sea ejecutable la resolución por la que se impone la sanción o haya transcurrido el plazo para recurrirla.

Se crearon tres agencias autonómicas: en Madrid en el año 2001, en Cataluña en el año 2003 y en País Vasco en el 2004. La Agencia de Protección de Datos de la Comunidad de Madrid fue suprimida el 1 de enero de 2013 y sus funciones pasaron a ser asumidas por la Agencia Española de Protección de Datos.

Actualmente existen dos agencias autonómicas: la Autoridad Catalana de Protección de Datos y la Agencia Vasca de Protección de Datos.

Las mismas ejercen las funciones de control respecto de los ficheros de datos de carácter personal creados o gestionados por las Comunidades Autónomas y por la Administración Local de su ámbito territorial. Los ficheros privados de estas CC. AA. son competencia de la Agencia Española de Protección de Datos.

e) Delegado de protección de datos.

El delegado de protección de datos, "es una figura novedosa[27] y que viene regulada en el RGPD y la LOPDGDD, que se presenta como obligatoria cuando el tratamiento sea llevado a cabo por una autoridad u organismo público, con excepción de los tribunales que actúen en el ejercicio de su función judicial, o cuando las actividades del responsable del tratamiento o del encargado del tratamiento 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 cuando las actividades del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos, a los que añaden los datos biométricos dirigidos a identificar de manera inequívoca a una persona física*".*

- El RGPD en su artículo 37 establece que se deberá designar un delegado de protección de datos cuando:

a) el tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial;

b) 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

c) 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.

[27] Extracto de la Obra "Primer Congreso Nacional de DPOs. Wolters Kluwers". Pag 32 Davara Rodriguez, Miguel Ángel (2018) DPO: "Cuestiones de interés en materia de formación y certificación". *Madrid*.

2. Un grupo empresarial podrá nombrar un único delegado de protección de datos siempre que sea fácilmente accesible desde cada establecimiento.

3. Cuando el responsable o el encargado del tratamiento sea una autoridad u organismo público, se podrá designar un único delegado de protección de datos para varias de estas autoridades u organismos, teniendo en cuenta su estructura organizativa y tamaño.

La Ley Orgánica 3/2018 de 5 de diciembre[28], de protección de datos personales y garantía de los derechos digitales, ha contemplado esta figura en el capítulo III, del Título V, que bajo este epígrafe **"delegado de protección de datos**" art. 34 a 37 se añade, además: serán obligados a designar un DPD los siguientes:

a) los colegios profesionales y sus consejos generales
b) Los centros docentes que ofrezcan enseñanzas en cualquiera de los niveles establecidos en la legislación reguladores de derecho a la educación, así como las universidades públicas y privadas.
c) las entidades que exploten redes y presten servicios de comunicaciones electrónicas conforme a su legislación específica, cuando traten habitual y sistemáticamente datos personales a gran escala.[29]
d) Los prestadores de servicios de la sociedad de la información cuando elaboren a gran escala perfiles de los usuarios del servicio.
e) Las entidades incluidas en el artículo 1 de la ley 10/2014, de 26 de junio, de ordenación, supervisión y solvencia de entidades de crédito.
f) Los establecimientos financieros de crédito
g) Las entidades aseguradoras y reaseguradoras
h) Las empresas de servicios de inversión, reguladas por la legislación del mercado de valores.
i) Los distribuidores y comercializadores de energía eléctrica y los distribuidores y comercializadores de gas natural.
j) Las entidades responsables de ficheros comunes para la evaluación de la solvencia patrimonial y crédito o de los ficheros comunes para la gestión y prevención del fraude, incluyendo a los responsables de los ficheros regulados por la legislación de prevención de prevención del blanqueo de capitales y de la financiación del terrorismo.
k) Las entidades que desarrollen actividades de publicidad y prospección comercial, incluyendo las de investigación comercial y de mercados, cuando lleven a cabo tratamientos basados en las preferencias de los afectados o realicen actividades que impliquen la elaboración de perfiles de los mismos.

[28] https://www.boe.es/buscar/doc.php?id=BOE-A-2018-16673 Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, consulta 13/04/19

[29] http://www.lssi.gob.es/paginas/Index.aspx Ley de servicios de la sociedad de la información y del comercio electrónico.

l) Los centros sanitarios legalmente obligados al mantenimiento de las historias clínicas de los pacientes.
Se exceptúan los profesionales de la salud que, aun estando legalmente obligados al mantenimiento de las historias clínicas de los pacientes, ejerzan su actividad a título individual.

m) las entidades que tengan como uno de sus objetos la emisión de informes comerciales que puedan referirse a personas físicas.

n) Los operadores que desarrollen la actividad de juego a través de canales electrónicos, informáticos, telemáticos e interactivos, conforme a la normativa de regulación del juego.

ñ) las empresas de seguridad privada

o) las federaciones deportivas cuando traten datos de menores de edad.

2. Los responsables o encargados del tratamiento no incluidos en el párrafo anterior podrán designar de manera voluntaria un delegado de protección de datos, que quedará sometido a régimen establecido en el Reglamente (UE)2016/679 y en la LOPDGDD.

3. Los responsables y encargados del tratamiento comunicarán en el plazo de 10 días a la AEPD, la comunicación se podrá realizar a través de Sede Electrónica o en su caso, a las autoridades autonómicas de protección de datos, las designaciones, nombramientos y ceses de los delegados de protección de datos tanto en los supuestos en que se encuentren obligadas a su designación como en el caso en que sea voluntaria[30].

4. La AEPD y las autoridades autonómicas de protección de datos mantendrán, en el ámbito de sus respectivas competencias, una lista actualizada de delegados de protección de datos accesible por medios electrónicos.

5. Los DPO podrán establecer dedicación completa o a tiempo parcial, utilizando como criterio, el volumen de tratamientos, la categoría especial de los datos tratados o los riesgos para derechos o libertades de los interesados.

En su art.35 la LOPDGDD, nos remite al artículo 37.5 del RGPD, en el que se establece que se establecerán "mecanismos de certificación", no obstante, el DPO no necesita tener conocimientos específicos no obstante sí que se tendrán en consideración "la titulación universitaria que acredite conocimientos especializados de derecho y la práctica en materia de protección de datos*".*

En su artículo 36 que tiene como título Posición del delegado de protección de datos se establece, que entre otras funciones el delegado:

"1. Actuará como interlocutor del responsable o encargado del tratamiento ante la Agencia Española de Protección de Datos y las autoridades autonómicas de

[30] https://www.aepd.es/media/guias/guia-rapida-dpd.pdf guía sobre cómo se debe realizar la comunicación del DPO, realizada por la AEPD consulta 15/04/2019

protección de datos. El delegado podrá inspeccionar los procedimientos relacionados con el objeto de la presente ley orgánica y emitir recomendaciones en el ámbito de sus competencias.

2. Cuando se trate de una persona física integrada en la organización del responsable o encargado del tratamiento, 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 evitarse 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, no pudiendo oponer a este acceso el responsable o el encargado del tratamiento la existencia de cualquier deber de confidencialidad o secreto, incluyendo el previsto en el artículo 5 de esta ley orgánica.

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 administración y dirección del responsable o el encargado del tratamiento."

Por otro lado, destacar que la LOPDGDD excluye de la responsabilidad del régimen sancionador al DPD, art. 70 .2 "2. No será de aplicación al delegado de protección de datos el régimen sancionador establecido en este Título"

Pero hay matices respecto a esta figura que no están resueltos, aunque la figura DPD debe tener unos conocimientos cualificados, no se ha regulado nada al respecto de necesidad de colegiarse o incluso el salario y esto crea cierta incertidumbre.

III. AMBITO OBJETIVO Y SUBJETIVO. RGPD Y LOPDGDD.

Objeto del RGPD[31]

El RGPD se encarga de armonizar y homogeneizar las normas relativas a la protección de datos de carácter personal desde el punto de vista de los derechos de las personas físicas, como de las obligaciones de aquellos que intervienen en el tratamiento de dataos personales.

artículo 1 del RGPD, el Objeto de esta normativa común es establece “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”. Además, este precepto establece que no es otro el objetivo principal del Reglamento que establecer un sistema que defienda este derecho.

El Reglamento general de protección de datos supone la revisión de las bases legales del modelo europeo de protección de datos más allá de una mera actualización de la vigente normativa.” Procede a reforzar la seguridad jurídica y transparencia a la vez que permite que sus normas sean especificadas o restringidas por el Derecho de los Estados miembros en la medida en que sea necesario por razones de coherencia y para que las disposiciones nacionales sean comprensibles para sus destinatarios”.

Así, RGPD en su considerando 8, permite que la normativa de los Estado que desarrollan y especifican el presente reglamento, incorporen a ese derecho nacional “previsiones contenidas específicamente en el reglamento, en la medida en que sea necesario por razones de coherencia y comprensión”

Objeto de la LOPDGDD

Con respecto a la LOPDGDD, el artículo 1 establece que la ley orgánica tiene por objeto adaptar el ordenamiento jurídico español al RGPD y completar sus disposiciones, y garantizar igualmente los derechos digitales de los ciudadanos conforme al artículo 18.4 de la Constitución española. De esta manera, nuestra Constitución fue pionera en el reconocimiento del derecho fundamental a la protección de datos personales cuando dispuso que “la ley limitará el uso de la

[31]Vid. Este artículo hace especial incidencia en el ámbito de aplicación de la normativa en materia de protección de datos realizando una clara diferenciación en cada uno de los ámbitos, https://www.iberley.es/temas/objeto-ambito-aplicacion-rgpd-lopdgdd-62715 desarrollo del ámbito subjetivo y objetivo de la LOPDGDD Y RGPD, extraído de la obra IBERLEY “Objeto y ámbito de aplicación del Reglamento General de protección de Datos (RGPD) y de la LO 3/2018 de 5 de diciembre de protección de datos (LOPDGDD), COLEX, fecha consulta 13/04/2019

informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".

Ámbito de aplicación del RGPD

Para desarrollar el ámbito de aplicación se deben utilizar no solo los art. 2 y 3 del RGPD, que establecen el ámbito de aplicación material y territorial, sino que se debe atender a lo que sus "Considerandos" apuntan, estos son esenciales para interpretar ciertos puntos del desarrollo normativo del Reglamento.

Respecto al ámbito subjetivo, atendiendo a una delimitación positiva, su protección se despliega a las "personas físicas independientemente de su nacionalidad o de su lugar de residencia" tal como se determina en su Considerando 14, el mismo desarrollo una delimitación negativa estableciendo "tampoco resultará aplicable los datos de las empresas constituidas como personas jurídicas, incluido el nombre y la forma de la persona jurídica y sus datos de contacto".

El considerando 27, establece a su vez otra delimitación negativa, indicando que los datos de las personas fallecidas, sin embargo, abre la posibilidad de que sea la misma normativa nacional la que regule el tratamiento de los datos de aquellas.

Por lo que respecta al "ámbito territorial de aplicación, resulta necesario atender a lo dispuesto en el artículo 3 por cuanto que -como veremos- a través de este precepto se atribuye al Reglamento un efecto "extramuros" de las fronteras comunitarias."

Así, el citado artículo 3 extiende los efectos tuitivos del Reglamento más allá del territorio europeo.

En este sentido, el precepto es claro al señalar que el Reglamento se aplica:

- "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."

- al tratamiento de datos personales de interesados que se encuentren en la Unión por parte de un responsable o encargado no establecido en la Unión, cuando las actividades de tratamiento estén relacionadas con:

a) la oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si a estos se les requiere su pago, o

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

Pero, ¿cuándo podemos considerar que un responsable del tratamiento cuenta con un establecimiento en la Unión? Y en el caso de que ni el responsable, ni el encargado estén establecidos en territorio comunitario, ¿cómo determinar si las actividades de tratamiento están relacionadas con la oferta de bienes y servicios del interesado o con en el control del comportamiento de este?

Estas cuestiones se responden disgregando uno a uno los conceptos establecidos:

- ✓ Es en su considerando 22, donde el término establecimiento se define como “el ejercicio de manera efectiva y real de una actividad a través de modalidades estables” esta definición tiene mucha concordancia con la definición de la LINRN de establecimiento permanente en su art.13 a mi parecer.
- ✓ Otro punto que determina la “sujeción” al RGPD, en su considerando 23, en el caso de que el responsable o encargado NO esté establecido en la UE, es el ofrecimiento de servicios o bienes a interesados de estados miembros de la UE.

“destacar que el hecho de que desde la Unión pudiera accederse a la web del responsable o encargado, o la circunstancia de que se pudieran conocer datos de contacto del mismo, no supondrá “per se” motivo suficiente para considerar que se está tratando de realizar esa oferta de bienes y servicios. Ahora bien, existen determinados factores como el uso de una lengua o una moneda utilizada generalmente en uno o varios Estados miembros, o la mención de clientes o usuarios que residen en la Unión que -como nos indican el considerando 24- pueden revelar que responsable del tratamiento proyecta ofrecer bienes o servicios a interesados en la Unión”

- ✓ El último de los casos que destaca el RGPD en su considerando 24, se refiere a la consideración del comportamiento de esa actividad y de determinar si está orientado a tratar datos de los interesados de la UE, por ejemplo, elaboración de un perfil.

AMBITO MATERIAL

En relación al **ámbito material** de aplicación del Reglamento, nuevamente debemos de realizar un doble análisis atendiendo en primer lugar, al aspecto positivo y, en segundo término, a aquellas actividades de tratamiento que -por diferentes razones- no son reguladas por la norma comunitaria.

El artículo 2 del Reglamento determina que este será de aplicación tanto al tratamiento total o parcialmente automatizado de datos personales, como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero.

Este precepto señala algo que quizás pueda resultar obvio, y es que la protección que otorga el Reglamento a las personas debe de aplicarse tanto al tratamiento automatizado de datos personales, como a su tratamiento manual. En este sentido, el considerando 15 determina que "a fin de evitar que haya un grave riesgo de elusión, la protección de las personas físicas debe ser tecnológicamente neutra y no debe depender de las técnicas utilizadas."

Pues bien, la exigencia de que los derechos inherentes a la protección de datos resulten aplicables no solo al tratamiento automatizado, sino también al denominado tratamiento "manual" pudiera llevar a pensar que cualquier tipo de aproximación o utilización de datos de terceras personas constituye "tratamiento". Sin embargo, la jurisprudencia ha señalado que únicamente los tratamientos de datos no automatizados quedarán comprendidos en el ámbito de protección de la normativa en la medida que los datos de carácter personal se encuentren contenidos en un fichero estructurado[32].

Por su parte en la sentencia de 1 de octubre de 2008, tras referirse a los considerandos 15 y 27 de la Directiva 95/46 , se añade "la propia Directiva 95/46 refiere el ámbito de la protección que regula al tratamiento del dato, y en relación tanto con los tratamientos automatizados como respecto a los que no lo estén, siempre que en este caso los datos estén contenidos o se destinen a encontrarse contenidos en un fichero, entendido éste como un archivo estructurado según criterios específicos relativos a las personas que permitan acceder fácilmente a los datos personales."

En este mismo sentido, el considerando 15 del RGPD señala que *"los ficheros o conjuntos de ficheros, así como sus portadas, que no estén estructurados con arreglo a criterios específicos, no deben entrar en el ámbito de aplicación del*

[32] Así, la **Audiencia Nacional** ha señalado en diversas ocasiones (SAN, sec. 1ª, de 9-7-2009, ref. 274/2008) que "para que una actuación manual sobre datos personales (recogida, grabación, conservación, elaboración, modificación, bloqueo etc...) tenga la consideración de tratamiento de datos sujeto al sistema de protección de **la LOPD** es necesario, según criterio reiterado de la Sala, que dichos datos estén contenidos o destinados a ser contenidos en un fichero, esto es, en un conjunto estructurado u organizado de datos con arreglo a criterios determinados.

presente Reglamento". En consecuencia, la acumulación o depósito de datos de forma no estructurada, sin atender a un criterio de ordenación que pudiera permitir la búsqueda e identificación de los datos de una persona, no resultaría sometido al régimen tuitivo establecido en el RGPD.

Desde una perspectiva negativa -y atendiendo a lo dispuesto en el apartado 2º del citado artículo 2- el Reglamento no resulta aplicable 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;

Conforme se indica en los apartados a) y b) reproducidos, las actividades relativas a la seguridad nacional en tanto que resultan ser actividades excluidas del ámbito del Derecho de la Unión no estarían sometidas a las disposiciones del Reglamento. Asimismo, esta norma tampoco se aplicaría al tratamiento de datos de carácter personal por los Estados miembros en el ejercicio de las actividades relacionadas con la política exterior y de seguridad común de la Unión.

c) efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas;

Resulta necesario señalar que la Audiencia Nacional Sala ha declarado con reiteración (SAN 12 de mayo de 2011, Rec. 31/2010) en el derecho a la protección de datos de carácter personal quedan incluidos los datos de los profesionales individuales, como se deriva del artículo 2 del RD 1720/2007, de 21 de diciembre, y así se puso de manifiesto por el Tribunal Supremo en la Sentencia de 20 de febrero de 2007

En este mismo sentido se ha pronunciado la Audiencia Nacional en SSAN de 28 de abril de 2015 y de 12 de mayo de 2011 en las que ha tratado el problema de la aplicación o no de la normativa sobre protección de datos a aquellos supuestos referidos a personas físicas, pero que lleven a cabo una actividad mercantil o profesional, considerando que:

" (...)no puede concluirse que los empresarios individuales y profesionales estén en todo caso y en su conjunto excluidos del ámbito de protección de la LOPD, sino que se hace necesario diferenciar, aunque la línea divisoria sea difusa, cuando un dato del empresario o profesional, se refiere a la vida privada de la persona y cuando a la empresa o profesión, pues solo en el primer caso cabe aplicar la protección de la LO 15/1999".

Esta tarea de diferenciación puede basarse en dos criterios distintos y complementarios:

i. Uno, el criterio objetivo de la clase y la naturaleza de los datos tratados, según estén en conexión y se refieran a la esfera íntima y personal o a la esfera profesional de la actividad.
ii. Otro, el de la finalidad del tratamiento y circunstancias en que éste se desarrolla, criterio éste que operaría en aquellos casos en que alguno de los datos profesionales coincidiera con los datos particulares del profesional o empresario (por ej. coincidencia de domicilio privado con el de la empresa, o cuando no se pueda acreditar si una deuda es de la empresa o si es personal del interesado).”

Atendiendo al contenido del considerando 18 del RGPD, entre las actividades personales o domésticas cabe incluir la correspondencia y la llevanza de un repertorio de direcciones, o la actividad en las redes sociales y la actividad en línea realizada en el contexto de las citadas actividades. No obstante, el Reglamento si resultará de aplicación a los responsables o encargados del tratamiento que proporcionen los medios para tratar datos personales relacionados con tales actividades 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.

Con respecto a las actividades de tratamiento destinadas a tales fines, debemos de señalar que son objeto de regulación específica debiendo regirse por la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo.[33]

A respecto de esta cuestión desarrollare las siguientes cuestiones, ¿cabe posibilidad de aplicación directa de esta Directiva? ¿qué sucede cuando esa Directiva no se ha transpuesto? ¿Cuándo debió transponerse? a esta cuestión se intentará dar respuesta mediante la aportación de opiniones no exentas de controversia. En el punto de desarrollo normativo se apuntarán estas opiniones.

Por último, en relación con el **análisis del ámbito material de aplicación del Reglamento**, resulta necesario realizar una serie de precisiones:

En primer lugar, el RGPD resultará de aplicación sin perjuicio de la aplicación de la Directiva 2000/31/CE, norma esta cuyo objetivo es contribuir al correcto funcionamiento del mercado interior garantizando la libre circulación de los servicios de la sociedad de la información entre los Estados miembros.

Por otra parte, aunque el tratamiento de datos de carácter personal por parte de las instituciones, órganos y organismos de la Unión se regula por las disposiciones del Reglamento (CE) no 45/2001, el tratamiento de datos realizado

[33] Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo.

por las citadas instituciones deberá de adaptarse a los principios y normas del presente Reglamento de conformidad con su artículo 98.

Asimismo, debemos tener en cuenta que, aunque el Reglamento se aplica, entre otras, a las actividades de los tribunales y otras autoridades judiciales, en virtud del Derecho de la Unión o de los Estados miembros pueden especificarse las operaciones de tratamiento y los procedimientos de tratamiento en relación con el tratamiento de datos personales por los tribunales y otras autoridades judiciales.

Ámbito de aplicación de la LOPDGDD

Con respecto al ámbito de aplicación de la LO 3/2018, se establece que se aplicará lo dispuesto en los Título I a IX y en los artículos 89 a 94, a cualquier tratamiento de datos personales contenidos o destinados a ser incluidos en un fichero, ya sea total o parcialmente automatizado, así como no automatizado.

Se exceptúa su aplicación en el caso de:

- tratamientos excluidos del ámbito de aplicación del RGPD;

- tratamientos de datos de personas fallecidas, salvo lo indicado en el artículo 3; y

- tratamientos sometidos a normativa sobre protección en materias clasificadas.

En cuanto a 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, se regirán por lo dispuesto en su legislación específica si la hubiese, y supletoriamente por lo dispuesto en el RGPD y en la LOPDGDD.

En el caso de los tratamientos de datos llevados 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, que se regirán por el RGPD y la LOPDGDD, sin perjuicio de las disposiciones de la Ley Orgánica 6/1985, de 1 de julio[34], del Poder Judicial que le sean aplicables.

Con respecto a los **datos de las personas fallecidas**, la LOPDGDD destaca por su novedosa regulación, puesto que si bien el RGPD deja claro que no es de aplicación, la nueva Ley Orgánica española en su artículo 3, tras excluir del ámbito de aplicación de la ley su tratamiento, 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.

[34] Ley Orgánica 6/1985, de 1 de julio. LO del Poder Judicial.

Se permite igualmente su solicitud a las personas o instituciones a las que el fallecido hubiese designado expresamente para ello, así como, en el caso de menores, el ejercicio por parte de sus representantes legales o el Ministerio Fiscal (de oficio o a instancia de cualquier persona física o jurídica interesada).
En el caso de personas con discapacidad, además de sus representantes y del Ministerio Fiscal, también podrán ejercer estas facultades aquellos designados para el ejercicio de funciones de apoyo.
Evidentemente se exceptúa su aplicación si el fallecido lo hubiese prohibido expresamente o así lo estableciese una Ley.
Queda pendiente la publicación de un real decreto que establezca los requisitos y condiciones para acreditar la validez y vigencia de estos mandatos e instrucciones, y en su caso, el registro de los mismos.

IV. PRINCIPIO JURÍDICOS.

El art 5 del RGPD, recoge esos principios, algunos ya configurados y asentados con la anterior normativa, recordar que la LOPD y la directiva 95/46/CE ya contenía "principios en cuanto a la calidad de los datos" o "principios generales", ahora vienen encuadrados en el epígrafe "principios relativos al tratamiento de datos"

Art. 5.1. a) RGPD Principio de lealtad, licitud y transparencia: "los datos deben ser tratados de manera leal, lícita y transparente. En relación con el Considerando[35] 39: Todo tratamiento de datos personales debe ser lícito y leal. La AEPD establece que el tratamiento de datos personales ha de estar claramente definida, así como permitida por el ordenamiento jurídico, además establece que los datos no pueden tratarse de manera desleal o sin proporcionar toda la información necesaria sobre el objeto y fines de tratamiento, sus consecuencias posibles riesgos, obligando a los responsables a que ofrezcan mayor transparencia en el tratamiento de sus datos.

- Hay que resaltar que, aunque el consentimiento constituye la base legal directriz en el tratamiento de datos personales, no es la única y en ocasiones no es la más adecuada (especial referencia al uso del consentimiento como base legal del tratamiento de datos en la administración pública o en una relación laboral genera controversia) se hará alusión más adelante a esta peculiaridad. Esta base legal instruirá de legitimidad el tratamiento art. 6 RGPD.
- Principio de licitud. Base legal del tratamiento bajo esta premisa, el artículo 6RGPD establece que el tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:
    - a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos.
    - b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales.
    - c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento.
    - d) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física.
    - e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.
    - f) el tratamiento es 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

[35] ¿Qué es un Considerando? Cada una de las razones que apoyan o sirven de fundamento al texto de una ley o a una sentencia, auto, decreto o resolución. Recibe dicho nombre por ser ésta la palabra con que comienza-http://www.enciclopedia-juridica.com/d/considerando/considerando.htm.

que requieran la protección de datos personales, en particular cuando el interesado sea un niño.

- Lo dispuesto en la letra f) del párrafo primero no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones.

- Principio de transparencia. -considerando 39. Art. 5.1.a) el interesado debe conocer con claridad, los datos que se están recogiendo, utilizando, consultando o tratando, así como la medida en que dichos datos son o serán tratados. Pero la exigencia va más allá y además exige que se utilice un lenguaje, claro y sencillo.
- Principio de limitación: Tus datos personales serán recogidos para unos fines determinados, explícitos y legítimos, y no serán tratados de manera incompatible con otros fines.

Se prohíbe a su vez el tratamiento de datos incompatibles para el fin perseguido

- Principio de minimización de datos: se utilizarán los datos adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados. No es posible recabar otros datos que no sean necesarios para el fin que se persiguen, bajo ningún pretexto incluso que el servicio sea gratuito.

Ejemplo: me bajo aplicación que envejece mi rostro y con la excusa cedo datos sobre localización, almacenamiento, contactos o agenda, correos electrónicos asociados, etc.… Por tanto, ese tratamiento no sería válido.

Al hilo del principio de minimización se puede hacer alusión a diversas actividades que pueden vulnerar este principio, como el caso de publicación de notas en concursos públicos o simplemente en la evaluación de unos alumnos en la universidad. ¿qué datos deben publicarse? En muchas circunstancias se incumple taxativamente pues se pretende dar tal transparencia de los procesos que en ocasiones se publican más datos de los necesarios para cumplir con esta transparencia. A continuación, exponemos unos casos y la solución por parte de la AEPD:

❖ ¿Se puede publicar las notas de los aspirantes en una oposición de carácter público, se puede publicar las de los alumnos en una universidad, con nombre apellidos y DNI? Esta además afecta a publicaciones de Becas de alumnos en centros escolares, las cuales deben adoptar las siguientes medidas y además omitir datos sensibles en las listas de exposición pública.

- Publicación de actos administrativos por los interesados:

La Disposición adicional séptima de la LOPDGDD nos da la clave:

Identificación de los interesados en las notificaciones por medio de anuncios y publicaciones de actos administrativos.

1. Cuando sea necesaria la publicación de un acto administrativo que contuviese datos personales del afectado, se identificará al mismo mediante su nombre y apellidos, añadiendo cuatro cifras numéricas aleatorias del documento nacional de identidad, número de identidad de extranjero, pasaporte o documento equivalente.
2. Cuando la publicación se refiera a una pluralidad de afectados estas cifras aleatorias deberán alternarse. Cuando se trate de la notificación por medio de anuncios, particularmente en los supuestos a los que se refiere el artículo 44 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, se identificará al afectado exclusivamente mediante el número completo de su documento nacional de identidad, número de identidad de extranjero, pasaporte o documento equivalente.
3. Cuando el afectado careciera de cualquiera de los documentos mencionados en los dos párrafos anteriores, se identificará al afectado únicamente mediante su nombre y apellidos. En ningún caso debe publicarse el nombre y apellidos de manera conjunta con el número completo del documento nacional de identidad, número de identidad de extranjero, pasaporte o documento equivalente.

La AEPD emite un informe orientativo de cómo realizar dichas publicaciones, se muestra un extracto del mismo:

Para ello, han seleccionado aleatoriamente el grupo de cuatro cifras numéricas que se van a publicar para la identificación de los interesados en las publicaciones de actos administrativos.
El procedimiento para la determinación de forma aleatoria de las cuatro cifras numéricas a publicar del código de identificación de un interesado se realizó mediante el proceso de selección aleatoria en una bolsa opaca de una bola de entre cinco bolas numeradas del 1 al 5, realizado el 27 de febrero de 2019 en la AEPD.
La bola resultante fue la número 4, por lo tanto: La publicación de documento nacional de identidad, número de identidad de extranjero, pasaporte o documento equivalente podrá realizarse de la siguiente forma:
• Dado un DNI con formato 12345678X, se publicarán los dígitos que en el formato que ocupen las posiciones cuarta, quinta, sexta y séptima. En el ejemplo: ***4567**.
• Dado un NIE con formato L1234567X, se publicarán los dígitos que en el formato ocupen las posiciones, evitando el primer carácter alfabéticos, cuarta, quinta, sexta y séptima. En el ejemplo: ****4567*.
• Dado un pasaporte con formato ABC123456, al tener sólo seis cifras, se publicarán los dígitos que en el formato ocupen las posiciones, evitando los tres caracteres alfabéticos, tercera, cuarta, quinta y sexta. En el ejemplo: *****3456.

• Dado otro tipo de identificación, siempre que esa identificación contenga al menos 7 dígitos numéricos, se numerarán dichos dígitos de izquierda a derecha, evitando todos los caracteres alfabéticos, y se seguirá el procedimiento de publicar aquellos caracteres numéricos que ocupen las posiciones cuarta, quinta, sexta y séptima. Por ejemplo, en el caso de una identificación como: XY12345678AB, la publicación sería: *****4567***.

❖ Envío de correos electrónicos por parte de una AAPP sin copia oculta.

La casuística es muy diversa pero no por ello poco frecuente, en este caso se pone en evidencia clara que se debe de dar mayor importancia a esa educación digital y a trabajar en el desarrollo de programa educativo en TIC sobre todo desde un prisma de seguridad y privacidad, pues así evitaremos cometer este tipo de vulneraciones en materia de protección de datos. Este caso, RESOLUCIÓN: R/01625/2018 el Ayuntamiento de Avilés, que remitió un correo con todos los aspirantes a un curso de electricidad en el que no se ocultó el listado de correo electrónico del resto de destinatarios, AEPD consideró en esta resolución una revelación de datos de carácter persona y por tanto una infracción de carácter grave a la normativa de protección de datos. En su argumentación de fundamentos de derecho, hace alusión a la obligación de custodia de los datos de los responsables y de todos los que intervengan en la fase de tratamiento que se incardina en su art 10.

Señala también que la Audiencia Nacional también ha apuntado lo siguiente: “Este deber de sigilo 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 CE

A mi parecer, es característico q en su exposición, la Agencia no deja a un lado su carácter educador y señala cómo debieran enviarse ese tipo de correo y así no producir un quebranto a la normativa vigente. La Agencia indica “A este respecto, cuando al remitente del mensaje le sea exigible este deber de secreto, se considera preciso el recurso a una modalidad de envío que ofrecen los programas de correo electrónico disponibles en el mercado, la cual permite detallar las direcciones electrónicas de los destinatarios múltiples en un campo específico del encabezado del mensaje: el campo CCO (con copia oculta), en lugar del habitual CC.”

Por último, resuelve que debido a que es una AAPP pública la infracción que corresponde, es la contemplada en el art. 46 LOPD, recordando que además de esta resolución caben medidas disciplinarias.

- Principio de exactitud: los datos deben ser exactos y si fuera necesario actualizados, adoptándose medidas necesarias para que

se supriman o rectifiquen sin dilación los datos personales que sean inexactos respecto los fines para que se traten[36].

- Principio de plazo de conservación: Los datos personales serán mantenidos de forma que se permita la identificación de los interesados por un plazo de tiempo no superior al necesario para cumplir los fines de tratamiento.

Esto hace alusión a que el responsable en el momento de recabar de los datos deberá informar del período o criterios de conservación de tus datos personales.

Este principio enlaza también con una de las novedades de la normativa de protección de datos, se suprime la necesidad de dar de alta el fichero de tratamiento de datos en la AEPD, pero se hace necesario el Registro de Actividades de tratamiento (en el que aparecerá los datos que se tratan por el responsable y añade toda la información respecto a su destino y conservación, legitimación para su tratamiento, cesión a terceros, uso)[37]

[36] (Sentencia Avon, respecto la resolución de AEPD imposición de dos sanciones de 28.000 euros, falta de consentimiento e inexactitud, Audiencia Nacional, Sentencia 25 septiembre 2019) https://diariolaley.laleynext.es/content/Documento.aspx?params=H4sIAAAAAAAAEAMtMSbH1CjUwMDAzMTc2NzFWK0stKs7Mz7Mty0xPzStJBfEz0ypd8pNDKgtSbdMSc4pT1TKLHQsKivLLUlNsjQwMLQ0NDC0MDQ0MAKwec6lMAAAAWKE

[37]https://diariolaley.laleynext.es/content/Documento.aspx?params= D

V. MARCO JURIDICO

5.01 Normativa Europea [38]:

La protección de los datos personales y el respeto de la vida privada son derechos fundamentales importantes. El Parlamento Europeo ha insistido siempre en la necesidad de lograr un equilibrio entre el refuerzo de la seguridad y la tutela de los derechos humanos, incluida la protección de los datos y de la vida privada. Las nuevas normas en materia de protección de datos, que refuerzan los derechos de los ciudadanos y simplifican las normas para las empresas en la era digital, entraron en vigor en mayo de 2018.

Dichas normativas tienen su base jurídica en:

- ✓ Artículo 16 del Tratado de Funcionamiento de la Unión Europea (TFUE)13 de diciembre de 2007[39] (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.

- ✓ Artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea 18 de diciembre del 2000[40].
  - Artículo 7 Respeto de la vida privada y familiar Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones.
  - Artículo 8 Protección de datos de carácter personal 1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.

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. El respeto de estas normas quedara sujeto al control de una autoridad independiente.

[38] http://www.europarl.europa.eu/factsheets/es/sheet/157/la-proteccion-de-los-datos-personales,consulta 18/03/2019
[39] https://eur-lex.europa.eu/legal-content/es/ALL/?uri=CELEX%3A12012E%2FTXT18/03/2019
[40] http://www.europarl.europa.eu/charter/pdf/text_es.pdf18/03/2019

2. Consejo de Europa

a. El Convenio n. 108 de 1981

El Convenio n. 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 fue el primer instrumento internacional jurídicamente vinculante adoptado en el ámbito de la protección de datos. 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».

b. Convenio Europeo de Derechos Humanos (CEDH) El artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales (CEDH), de 4 de noviembre de 1950, consagra el derecho al respeto de la vida privada y familiar: «Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia».

3.Otros instrumentos legislativos en la Unión en materia de protección de datos:

- Es la **Directiva 95/46/CE** [41]relativa a la protección de datos (sustituida por el Reglamento general de protección de datos en mayo de 2018), la Directiva 2002/58/CE (modificada en 2009; actualmente se trabaja en una nueva propuesta) sobre la privacidad y las comunicaciones electrónicas, la Directiva 2006/24/CE sobre la conservación de datos (declarada inválida por el Tribunal de Justicia de la Unión Europea el 8 de abril de 2014 al constituir una injerencia de especial gravedad en la vida privada y la protección de datos) y el Reglamento (CE) nº 45/2001 relativo al tratamiento de datos personales por las instituciones y los organismos comunitarios (actualmente se trabaja en una nueva propuesta), así como instrumentos pertenecientes al antiguo tercer pilar, como la Decisión Marco del Consejo 2008/977/JAI, de 27 de noviembre de 2008, relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal (sustituida por la Directiva sobre protección de datos en el ámbito penal en mayo de 2018).

[41] Recordar que las fuentes del Derecho comunitarias son el derecho originario y el derivado, dentro del derivado están los Reglamentos que son de aplicación general y obligado cumplimiento por todos los estados miembros no necesitan de transposición interna normativa, tienen efectos desde su publicación.
Las directivas que tienen efectos sobre los estados que se pronuncian, aunque su obligación se aplica solo respecto al objeto de las misma dejando cierta discrecionalidad a los Estados de como incorporarla a su normativa interna, en caso de no transposición en el plazo establecido el Estado tendrá responsabilidad sobre el incumplimiento; la comisión intentará mediante comunicaciones que esta se cumpla y si no fuera así se trasladará al tribunal de la comunidad europea. Se podrá además invocar por los justiciables la aplicación directa de la misma por los tribunales internos.

- **El <u>Reglamento general de protección de datos RGP 2016/679</u>**[42] supone la revisión de las bases legales del modelo europeo de protección de datos más allá de una mera actualización de la vigente normativa. Procede a reforzar la seguridad jurídica y transparencia a la vez que permite que sus normas sean especificadas o restringidas por el Derecho de los Estados miembros en la medida en que sea necesario por razones de coherencia y para que las disposiciones nacionales sean comprensibles para sus destinatarios.

✓ El Reglamento general de protección de datos, 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), entró en vigor desde el 25 mayo de 2018.

✓ El reglamento de protección de datos contiene XI Capítulos divididos en:

1. Disposiciones Generales
2. Principios
3. Derechos de los Interesados
4. Responsable del Tratamiento y Encargado del Tratamiento
5. Transferencia a Terceros Países u Organizaciones Internacionales
6. Autoridades de Control
7. Cooperación y Coherencia
8. Recursos
9. Responsabilidad y Sanciones
10. Situaciones Específicas de Tratamiento
11. Actos delegados y Actos ejecución
12. Disposiciones finales

Como novedades significativas el nuevo Reglamento de Protección de datos, introduce la figura <u>de delegado de protección de datos</u>, realización de evaluaciones de impacto como ejemplo de una actividad de control más proactiva, se trata no solo de resolver los problemas cuando surjan sino además de prevenir los problemas antes de que surjan y en todo caso cuando surjan poder minimizar los daños.

Por otro lado, el RGPD acota claramente mediante los principios, una serie de requisitos para que el tratamiento de datos sea lícito, para eso establece el Reglamento que deben cumplirse las siguientes condiciones:

a. Que el interesado de su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos
b. Que el tratamiento sea necesario para la ejecución de un contrato en el que el interesado es parte; (…)

[42] https://www.boe.es/eli/es/lo/2018/12/05/3 consulta el 13/04/2019

El consentimiento se configura como pieza fundamental para el tratamiento de datos de carácter personal. Así cuando dicho tratamiento se base en el consentimiento del interesado, el responsable del tratamiento deberá ser capaz de demostrar que aquel consintió el tratamiento de sus datos personales mediante una manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta. Esto forma parte de esa responsabilidad proactiva. Además, esa información previa debe ser por escrito y servirse de manera concisa, transparente, inteligible, de fácil acceso y con lenguaje claro y sencillo. Por parte de la Agencia de Protección de datos se realice por capas para facilitar la comprensión de la extensión de su consentimiento, la agencia ha publicado una guía para el cumplimiento de la obligación de informar optando por un modelo de información por capas o niveles y explicando con detalle cómo debería efectuarse el deber de información al interesado. [43]

No obstante en esa información debe aparecer la identidad y contacto del responsable de datos, si lo hubiera el del delegado de protección de datos, los fines del tratamiento y el destino así como la base jurídica del tratamiento, intereses legítimos del tratamiento, los destinatarios o categorías de destinatarios y plazo durante el cual se utilizaran los datos personales y los criterios para determinar este plazo, la existencia del derecho a solicitar al responsable el ejercicio de los derechos que le asisten, posibilidad de retirar el consentimiento, derecho a presentar una reclamación ante la autoridad de control y si existe decisiones automatizadas para la elaboración de perfiles, así como las posibles transferencias internacionales de datos de carácter personal a un tercer país u organización.

El objetivo de las normas es proteger a todos los ciudadanos de la Unión frente a las violaciones de la privacidad y de los datos personales en un mundo cada vez más basado en los datos, creando al mismo tiempo un marco más claro y coherente para las empresas.

[43] https://www.aepd.es/media/guias/guia-modelo-clausula-informativa.pdf consulta 13/04/2019

Como hemos expresado el responsable debe informar al ciudadano de los derechos que le asisten, pero ¿cuáles son estos derechos?

En concreto, los derechos del interesado en materia de protección de datos personales a los que atenderemos son los relativos a:

- • Derecho de acceso del interesado. Art 15 RGPD
- • Derecho de rectificación. art 16 RGPD
- • Derecho de supresión («el derecho al olvido»). art.17 RGPD
- • Derecho a la limitación del tratamiento (art.18 RGPD).
- • Derecho a la portabilidad de los datos (art.20 RGPD).
- • Derecho de oposición (art.21 RGPD).
- • Decisiones individuales automatizadas, incluida la elaboración de perfiles (art.22 RGPD)

Las nuevas normas se aplican a todas las empresas que operan en la Unión, incluso si tienen su sede fuera de la UE. Asimismo, será posible imponer medidas correctoras, tales como advertencias y órdenes, o sanciones a las empresas que infrinjan las normas.

Por último, señalar otra de la Directivas de aplicación:

La Directiva sobre protección de datos en el ámbito penal 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, entró en vigor en mayo de 2018.

La Directiva protege el derecho fundamental de los ciudadanos a la protección de datos cuando los utilizan las autoridades policiales. Garantiza que los datos personales de víctimas, testigos y sospechosos de delitos sean debidamente protegidos, y facilita la cooperación transfronteriza en la lucha contra la delincuencia y el terrorismo.

Dicha directiva no se transpuso en su momento 6 mayo de 2018 y por tanto se desprende los siguiente:

> [44] "Se plantea como posible efecto directo vertical de la Directiva 2016/680 en relación con los derechos reconocidos por la misma a los particulares frente a los poderes públicos, siempre que concurran los presupuestos a tal

[44] https://elderecho.com/la-proteccion-datos-personales-proceso-penal-directiva-2016-680

efecto exigidos por la jurisprudencia del TJUE, que recoge el propio TC español[45]":

- Que el Estado miembro de la UE no haya transpuesto la directiva antes del plazo correspondiente; lo que ocurre en relación con la Directiva 2016/680.
- Que la aplicación se refiera a disposiciones incondicionales y suficientemente claras y precisas, que contemplen derechos a los ciudadanos

"Cabe recordar que el **efecto directo vertical** reconoce la posibilidad de que un particular invoque normas contenidas en una Directiva no ejecutada en el Estado del que es nacional, porque su efecto útil se vería debilitado si se impidiera a los justiciables hacerlo valer en justicia y a las jurisdicciones nacionales tomarlo en consideración en cuanto elemento de Derecho *comunitario.*

Como recuerda Pérez Van Kappel[46], "el Estado miembro que no haya adaptado dentro del plazo las medidas de ejecución que impone una directiva, no puede oponer a los particulares su propio incumplimiento de las obligaciones que la directiva implica".

"En todo caso, pese a la falta de transposición, la Directiva no transpuesta despliega una serie de efectos en la aplicación judicial, y ello por cuanto las obligaciones derivadas de la directiva recaen sobre todos los órganos del Estado, cada uno dentro de su respectiva competencia, incluidos los órganos jurisdiccionales. De esta forma, los tribunales internos están obligados a contribuir al cumplimiento por parte del Estado de los deberes impuestos por una Directiva, ya sea a través de la aplicación directa de la propia Directiva (efecto directo), o ya sea mediante la interpretación del Derecho interno de conformidad con el contenido de la Directiva (principio de interpretación conforme)[47].

---

[45] La STC 30-1-16 se refiere al efecto directo del art.7 de la Directiva 2012/13/UE, de 22 mayo 2012 desde la fecha en que expiró el plazo para su transposición (2 de junio de 2014), hasta la de la entrada en vigor de la LO 5/2015, de 27 abril, que llevó a cabo este último cometido. Afirma expresamente la STC que **«no cabe rechazar tampoco la posibilidad de que una Directiva comunitaria que no haya sido transpuesta dentro de plazo por el legislador español, o que lo haya sido de manera insuficiente o defectuosa, pueda ser vinculante en cuanto contenga disposiciones incondicionales y suficientemente precisas en las que se prevean derechos para los ciudadanos, incluyendo aquellos de naturaleza procesal que permitan integrar por vía interpretativa el contenido esencial de los derechos fundamentales, al haberse incorporado por vía de la jurisprudencia del Tribunal de Justicia de la Unión Europea, al acervo comunitario»**

[46] Antonio Pérez Van Kappel, que cita la Sentencia de 5-4-79 (Ratti) -, «El efecto directo del Derecho de la Unión Europea», Cuadernos Digitales de Formación, Espacio judicial europeo social. III Edición (2013-2014), Consejo General del Poder Judicial

[47] Como razona Mangas Martín, «ante la falta de transposición, o en caso de transposición incorrecta por los poderes públicos competentes, se traslada a los jueces, también órganos del Estado, la obligación de tomar las medidas necesarias para alcanzar en el litigio concreto el resultado querido por la directiva, ya tengan efecto directo sus disposiciones o no lo tengan» «Las relaciones entre el Derecho Comunitario y el Derecho interno de los Estados miembros a la luz de la Jurisprudencia del Tribunal de Justicia», dentro de la obra colectiva El

5.02 Normativa española:

a) <u>La constitución española especifica en su art. 18.4 de la Constitución Española:</u>

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.

De esta manera, nuestra Constitución fue pionera en el reconocimiento del derecho[48] fundamental a la protección de datos personales cuando dispuso 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». Se hacía así eco de los trabajos desarrollados desde finales de la década de 1960 en el Consejo de Europa y de las pocas disposiciones legales adoptadas en países de su entorno.

<u>b) Sentencias del Tribunal constitucional:</u>

El Tribunal Constitucional señaló en su Sentencia 94/1998[49], de 4 de mayo, que nos encontramos ante un derecho fundamental a la protección de datos 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, el derecho a la protección de datos se configura como una facultad del ciudadano para oponerse a que determinados datos personales sean usados para fines distintos a aquel que justificó su obtención.*

Por su parte, en la Sentencias 290 y 292/2000, lo considera como un derecho autónomo e independiente que 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.

A nivel legislativo, la concreción y desarrollo del derecho fundamental de protección de las personas físicas en relación con el tratamiento de datos personales tuvo lugar en sus orígenes mediante la aprobación de la Ley Orgánica 5/1992, de 29 de octubre, reguladora del tratamiento automatizado de datos personales, conocida como LORTAD.

La Ley Orgánica 5/1992 fue reemplazada por la Ley Orgánica 15/1999, de 5 de diciembre, de protección de datos personales, a fin de trasponer a nuestro derecho a 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

Derecho Comunitario Europeo y su aplicación judicial, editado por el CGPJ, la Universidad de Granada y la editorial Civitas, Madrid, 1993, pág. 81

[48] Preámbulo de la ley 3/2018 de 3 de diciembre, LOPDGDD https://www.boe.es/eli/es/lo/2018/12/05/3/con consultada el 13/04/2019

[49] https://www.boe.es/boe/dias/1998/06/09/pdfs/T00008-00013.pdf sentencia TC 94/1998

respecta al tratamiento de datos personales y a la libre circulación de estos datos.

c) Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD)

La ley orgánica[50] en su preámbulo delimita que esta ley nace no solo fruto de una actualización sino de una adaptación para conferir y reforzar de una mejor seguridad jurídica y permitir que esta normativa sea comprensible a sus destinatarios.

Así, el Reglamento general de protección de datos contiene un buen número de habilitaciones, cuando no imposiciones, a los Estados miembros, a fin de regular determinadas materias, permitiendo incluso en su considerando 8, y a diferencia de lo que constituye principio general del Derecho de la Unión Europea que cuando sus normas deban ser especificadas, interpretadas o, excepcionalmente, restringidas por el Derecho de los Estados miembros, estos tengan la posibilidad de incorporar al derecho nacional previsiones contenidas específicamente en el reglamento, en la medida en que sea necesario por razones de coherencia y comprensión. El reglamento se presenta como un instrumento normativo tedioso en su lectura y muy extenso, sus considerandos pese a ser tremendamente útiles en cuanto a la comprensión del texto no debe de interpretarse más allá y no hay que olvidar que no todos están incluidos en el instrumento normativo.

En definitiva, el principio de seguridad jurídica obliga a que la normativa interna que resulte incompatible con el Derecho de la Unión Europea quede definitivamente eliminada «mediante disposiciones internas de carácter obligatorio que tengan el mismo valor jurídico que las disposiciones internas que deban modificarse» (Sentencias del Tribunal de Justicia de 23 de febrero de 2006, asunto Comisión vs. España; de 13 de julio de 2000, asunto Comisión vs. Francia; y de 15 de octubre de 1986, asunto Comisión vs. Italia).

Por último, los reglamentos, pese a su característica de aplicabilidad directa, en la práctica pueden exigir otras normas internas complementarias para hacer plenamente efectiva su aplicación. En este sentido, más que de incorporación cabría hablar de «desarrollo» o complemento del Derecho de la Unión Europea de la nueva ley orgánica de protección de datos 3/2018.

ESTRUCTURA:

Esta ley orgánica consta de noventa y siete artículos estructurados en diez títulos, veintidós disposiciones adicionales, seis disposiciones transitorias, una disposición derogatoria y dieciséis disposiciones finales.

[50] https://www.boe.es/eli/es/lo/2018/12/05/3/con LOPDGDD estructura principal de la norma y resumen de los propósitos de desarrollo de cada uno de los títulos, fecha de consulta 13/04/2019

i. El Título I, relativo a las disposiciones generales, comienza regulando el objeto de la ley orgánica, que es, conforme a lo que se ha indicado, doble.

- primer lugar, se pretende lograr la adaptación del ordenamiento jurídico español al RGPD y completar sus disposiciones. A su vez establecer el derecho fundamental 18.4. Las comunidades autónomas ostentan competencias de desarrollo normativo y ejecución del derecho fundamental a la protección de datos personales en su ámbito de actividad y a las autoridades autonómicas de protección de datos que se creen les corresponde contribuir a garantizar este derecho fundamental de la ciudadanía.
- segundo lugar, es también objeto de la ley garantizar los nuevos derechos digitales de la ciudadanía, al amparo de lo dispuesto en el 18.4 CE.

Destaca la novedosa regulación de los datos referidos a las personas fallecidas, pues, 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 (Testamento digital) art96.

Derecho de acceso universal a internet (art. 81), derecho seguridad digital (art. 82), derecho a la educación digital art.83, protección de los menores en internet (art. 84 y 92), derecho de rectificación por internet (art. 85), derechos digitales en el ámbito laboral (art. 87 a 91), derecho a olvido (art. 93 y 94), derecho de portabilidad en servicios de redes sociales y equivalentes (art. 95)

ii. En el Título II, «Principios de protección de datos»,

Se regulan asimismo las posibles habilitaciones legales para el tratamiento fundadas en el cumplimiento de una obligación legal exigible al responsable.

Se podrán igualmente imponer condiciones especiales al tratamiento, tales como la adopción de medidas adicionales de seguridad u otras, cuando ello derive del ejercicio de potestades públicas o del cumplimiento de una obligación legal y solo podrá considerarse fundado en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable, en los términos previstos en el reglamento europeo, cuando derive de una competencia atribuida por la ley. Y se mantiene la prohibición de consentir tratamientos con la finalidad principal de almacenar información identificativa de determinadas categorías de datos especialmente protegidos, lo que no impide que los mismos puedan ser objeto de tratamiento en los demás supuestos previstos en el **Reglamento (UE) 2016/679.**

También en relación con el tratamiento de categorías especiales de datos, el artículo 9.2 consagra el principio de reserva de ley para su habilitación en los supuestos previstos en el Reglamento (UE) 2016/679. Dicha previsión no sólo alcanza a las disposiciones que pudieran adoptarse en el futuro, sino que permite dejar a salvo las distintas habilitaciones legales actualmente existentes, tal y como se indica específicamente, respecto de la legislación sanitaria y aseguradora, en la disposición adicional decimoséptima. El Reglamento general de protección de datos no afecta a dichas habilitaciones, que siguen plenamente

vigentes, permitiendo incluso llevar a cabo una interpretación extensiva de las mismas, como sucede, en particular, en cuanto al alcance del consentimiento del afectado o el uso de sus datos sin consentimiento en el ámbito de la investigación biomédica. A tal efecto, el apartado 2 de la Disposición adicional decimoséptima introduce una serie de previsiones encaminadas a garantizar el adecuado desarrollo de la investigación en materia de salud, y en particular la biomédica, ponderando los indudables beneficios que la misma aporta a la sociedad con las debidas garantías del derecho fundamental a la protección de datos.

iii. **El Título III, dedicado a los derechos de las personas,**

adapta al Derecho español el principio de transparencia en el tratamiento del reglamento europeo, que regula el derecho de los afectados a ser informados acerca del tratamiento y recoge la denominada «información por capas» ya generalmente aceptada en ámbitos como el de la videovigilancia o la instalación de dispositivos de almacenamiento masivo de datos (tales como las «cookies»), facilitando al afectado la información básica, si bien, indicándole una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata a la restante información.

Se hace uso en este Título de la habilitación permitida por el considerando 8 del Reglamento (UE) 2016/679para complementar su régimen, garantizando la adecuada estructura sistemática del texto. A continuación, la ley orgánica contempla los derechos de acceso, rectificación, supresión, oposición, derecho a la limitación del tratamiento y derecho a la portabilidad.

iv. **En el Título IV se recogen «Disposiciones aplicables a tratamientos concretos»,**

incorporando una serie de supuestos que en ningún caso debe considerarse exhaustiva de todos los tratamientos lícitos. Dentro de ellos cabe apreciar, en primer lugar, aquellos respecto de los que el legislador establece una presunción «iuris tantum» de prevalencia del interés legítimo del responsable cuando se lleven a cabo con una serie de requisitos, lo que no excluye la licitud de este tipo de tratamientos cuando no se cumplen estrictamente las condiciones previstas en el texto, si bien en este caso el responsable deberá llevar a cabo la ponderación legalmente exigible, al no presumirse la prevalencia de su interés legítimo. Junto a estos supuestos se recogen otros, tales como la videovigilancia, los ficheros de exclusión publicitaria o los sistemas de denuncias internas en que la licitud del tratamiento proviene de la existencia de un interés público, en los términos establecidos en el artículo 6.1.e) del Reglamento (UE) 2016/679. Finalmente, se hace referencia en este Título a la licitud de otros tratamientos regulados en el Capítulo IX del reglamento, como los relacionados con la función estadística o con fines de archivo de interés general. En todo caso, el hecho de que el legislador se refiera a la licitud de los tratamientos no enerva la obligación de los responsables de adoptar todas las medidas de responsabilidad activa establecidas en el Capítulo IV del reglamento europeo y en el Título V de esta ley orgánica.

v. **El Título V se refiere al responsable y al encargado del tratamiento**.

Es preciso tener en cuenta que la mayor novedad que presenta el Reglamento (UE) 2016/679 es la evolución de un modelo basado, fundamentalmente, en el control del cumplimiento a otro que descansa en el principio de responsabilidad

activa, lo que exige una previa valoración por el responsable o por el encargado del tratamiento del riesgo que pudiera generar el tratamiento de los datos personales para, a partir de dicha valoración, adoptar las medidas que procedan. Con el fin de aclarar estas novedades, la ley orgánica mantiene la misma denominación del Capítulo IV del Reglamento, dividiendo el articulado en cuatro capítulos dedicados, respectivamente, a las medidas generales de responsabilidad activa, al régimen del encargado del tratamiento, a la figura del delegado de protección de datos y a los mecanismos de autorregulación y certificación. La figura del delegado de protección de datos adquiere una destacada importancia en el Reglamento (UE) 2016/679 y así lo recoge la ley orgánica, que parte del principio de que puede tener un carácter obligatorio o voluntario, estar o no integrado en la organización del responsable o encargado y ser tanto una persona física como una persona jurídica. La designación del delegado de protección de datos ha de comunicarse a la autoridad de protección de datos competente. La Agencia Española de Protección de Datos mantendrá una relación pública y actualizada de los delegados de protección de datos, accesible por cualquier persona. Los conocimientos en la materia se podrán acreditar mediante esquemas de certificación. Asimismo, no podrá ser removido, salvo en los supuestos de dolo o negligencia grave. Es de destacar que el delegado de protección de datos permite configurar un medio para la resolución amistosa de reclamaciones, pues el interesado podrá reproducir ante él la reclamación que no sea atendida por el responsable o encargado del **tratamiento.**

vi. **El Título VI, relativo a las transferencias internacionales de datos**, procede a la adaptación de lo previsto en el Reglamento (UE) 2016/679 y se refiere a las especialidades relacionadas con los procedimientos a través de los cuales las autoridades de protección de datos pueden aprobar modelos contractuales o normas corporativas vinculantes, supuestos de autorización de una determinada transferencia, o información previa.

vii. **El Título VII se dedica a las autoridades de protección de datos**, que siguiendo el mandato del Reglamento (UE) 2016/679 se han de establecer por ley nacional. Manteniendo el esquema que se venía recogiendo en sus antecedentes normativos, la ley orgánica regula el régimen de la Agencia Española de Protección de Datos y refleja la existencia de las autoridades autonómicas de protección de datos y la necesaria cooperación entre las autoridades de control. La Agencia Española de Protección de Datos se configura como una autoridad administrativa independiente con arreglo a la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, que se relaciona con el Gobierno a través del Ministerio de Justicia.

viii. **El Título VIII regula el «Procedimientos en caso de posible vulneración de la normativa de protección de datos»**.

El Reglamento (UE) 2016/679 establece un sistema novedoso y complejo, evolucionando hacia un modelo de «ventanilla única» en el que existe una autoridad de control principal y otras autoridades interesadas. También se establece un procedimiento de cooperación entre autoridades de los Estados miembros y, en caso de discrepancia, se prevé la decisión vinculante del Comité Europeo de Protección de Datos. En consecuencia, con carácter previo a la tramitación de cualquier procedimiento, será preciso determinar si el tratamiento tiene o no carácter transfronterizo y, en caso de tenerlo, qué autoridad de protección de datos ha de considerarse principal.

La regulación se limita a delimitar el régimen jurídico; la iniciación de los procedimientos, siendo posible que la Agencia Española de Protección de Datos remita la reclamación al delegado de protección de datos o a los órganos o entidades que tengan a su cargo la resolución extrajudicial de conflictos conforme a lo establecido en un código de conducta; la inadmisión de las reclamaciones; las actuaciones previas de investigación; las medidas provisionales, entre las que destaca la orden de bloqueo de los datos; y el plazo de tramitación de los procedimientos y, en su caso, su suspensión. Las especialidades del procedimiento se remiten al desarrollo reglamentario.

ix. **El Título IX, que contempla el régimen sancionador**,

parte de que el Reglamento (UE) 2016/679 establece un sistema de sanciones o actuaciones correctivas que permite un amplio margen de apreciación. En este marco, la ley orgánica procede a describir las conductas típicas, estableciendo la distinción entre infracciones muy graves, graves y leves, tomando en consideración la diferenciación que el Reglamento general de protección de datos establece al fijar la cuantía de las sanciones. La categorización de las infracciones se introduce a los solos efectos de determinar los plazos de prescripción, 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. La ley orgánica regula los supuestos de interrupción de la prescripción partiendo de la exigencia constitucional del conocimiento de los hechos que se imputan a la persona, pero teniendo en cuenta la problemática derivada de los procedimientos establecidos en el reglamento europeo, en función de si el procedimiento se tramita exclusivamente por la Agencia Española de Protección de Datos o si se acude al procedimiento coordinado del artículo 60 del Reglamento general de protección de datos.

El Reglamento (UE) 2016/679 establece amplios márgenes para la determinación de la cuantía de las sanciones. La ley orgánica aprovecha la cláusula residual del artículo 83.2 de la norma europea, referida a los factores agravantes o atenuantes, para aclarar que entre los elementos a tener en cuenta podrán incluirse los que ya aparecían en el artículo 45.4 y 5 de la Ley Orgánica 15/1999, y que son conocidos por los operadores jurídicos.

x. **Finalmente, el Título X de esta ley acomete la tarea de reconocer y garantizar un elenco de derechos digitales de los ciudadanos conforme al mandato establecido en la Constitución**.

En particular, son objeto de regulación los derechos y libertades predicables al entorno de Internet como la neutralidad de la Red y el acceso universal o los derechos a la seguridad y educación digital, así como los derechos al olvido, a la portabilidad y al testamento digital.

Ocupa un lugar relevante el reconocimiento del derecho a la desconexión digital en el marco del derecho a la intimidad en el uso de dispositivos digitales en el ámbito laboral y la protección de los menores en Internet.

Finalmente, resulta destacable la garantía de la libertad de expresión y el derecho a la aclaración de informaciones en medios de comunicación digitales.

Las disposiciones adicionales se refieren a cuestiones como las medidas de seguridad en el ámbito del sector público, protección de datos y transparencia y acceso a la información pública, cómputo de plazos, autorización judicial en materia de transferencias internacionales de datos, la protección frente a

prácticas abusivas que pudieran desarrollar ciertos operadores, o los tratamientos de datos de salud, entre otras.

De conformidad con la disposición adicional decimocuarta, la normativa relativa a las excepciones y limitaciones en el ejercicio de los derechos que hubiese entrado en vigor con anterioridad a la fecha de aplicación del reglamento europeo 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, seguirá vigente en tanto no sea expresamente modificada, sustituida o derogada. No obstante, el art 24 de la citada ley fue declarado inconstitucional por sentencias del Tribunal Constitucional ya citadas la 290 y 292 del 2000.

Así, por ejemplo, en virtud de la referida disposición adicional, las Administraciones tributarias responsables de los ficheros de datos con trascendencia tributaria a que se refiere el artículo 95 de la Ley 58/2003, de 17 de diciembre, General Tributaria, podrán, en relación con dichos datos, denegar el ejercicio de los derechos a que se refieren los artículos 15 a22 del Reglamento (UE) 2016/679, 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.

Las disposiciones transitorias están dedicadas, entre otras cuestiones, al estatuto de la Agencia Española de Protección de Datos, el régimen transitorio de los procedimientos o los tratamientos sometidos a la Directiva (UE) 2016/680. Se recoge una disposición derogatoria y, a continuación, figuran las disposiciones finales sobre los preceptos con carácter de ley ordinaria, el título competencial y la entrada en vigor.

Asimismo, se introducen las modificaciones necesarias de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil y la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa, la Ley Orgánica, 6/1985, de 1 de julio, del Poder Judicial, la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General (repetir que el art. 58 bis se declaró inconstitucional), la Ley 14/1986, de 25 de abril, General de Sanidad, 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 y la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

Finalmente, y en relación con la garantía de los derechos digitales, también se introducen modificaciones en la Ley Orgánica 2/2006, de 3 de mayo, de Educación, la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades, así como en el Texto Refundido de la Ley del Estatuto de los Trabajadores y en el Texto Refundido de la Ley del Estatuto Básico del Empleado Público.

VI. CUADRO COMPARATIVO DE LAS NORMAS[51]

RGPD	LOPDGDD
CAPÍTULO I - Disposiciones generales	TÍTULO I. Disposiciones generales
Artículo 1. Objeto.	Artículo 1. Objeto de la ley
Artículo 2. Ámbito de aplicación material.	Artículo 2. Ámbito de aplicación de los Títulos I a IX y de los artículos 89 a 94.
Artículo 3. Ámbito territorial. Considerandos 22 a 25.	
Artículo 4. Definiciones. Considerandos 26, 28 a 30, 34 a 37	
CAPÍTULO II – Principios art.5 RGPD. Considerando 39 Licitud, lealtad y transparencia/ fin legítimo y explícitos/ adecuados y pertinentes y limitados/ exactos y actualizados/seguridad adecuada para evitar su acceso no autorizado o ilícito y contra su pérdida, destrucción o daño accidental/ bases para esa licitud art. 6 “Licitud tratamiento” / condiciones consentimiento art.7 / consentimientos del niño/tratamiento art.8. Considerando 32,42 y 43 / categorías especiales de datos (coincide con la ley en su número art.9) Considerandos 51 a 56/ tratamiento datos relativos condenas e infracciones penales/ tratamiento que no requiere identificación	TÍTULO II. Principios de protección de datos. Art.4 y 5. DA7 (“Identificación de los interesados en las notificaciones y publicaciones de actos administrativos “y DA8(“Potestad de verificación de las Administraciones públicas) Exactitud/Deber de confidencialidad/Tratamiento basado el consentimiento art.7 y 92. Considerando 38 / consentimientos menores/ Art. 8 tratamiento obligación legal, interés público o ejercicio de poderes públicos.DA9 y DA10/DF12/categorías especiales datos/ tratamiento datos (art.9) DA17(Datos especiales de salud)

[51] http://www.privacidadlogica.es/crossover-entre-el-rgpd-y-la-nueva-lopd/ Crossover LOPD Y RGPD, por Publicado el 13 de diciembre de 2018 por Francisco Javier Sempere

CAPITULO III DERECHOS INTERESADO	TITULO III. DERECHOS PERSONAS
SECCIÓN1. TRANSPARENCIA	CAP.I. TRANSPARENCIA
SECCIÓN2. INFORMACIÓN Y ACCESO A LOS DATOS PERSONALES Distingue dos circunstancias que los datos se obtengan de interesado art.13 y por tanto tienen derecho a una información Y que no se obtenga del interesado art.14 otra información Derecho acceso15,	CAP2. EJERCICIO DE DERECHOS Art.12disposicion generales/ 13. acceso, rectificación14., supresión15, limitación16, portabilidad17, oposición 18
Sección 3. Art. 16 derecho rectificación/ art.17 derecho supresión “olvido” / limitación 18/	
Obligación notificación relativa a la rectificación o supresión de datos personales o la limitación del tratamiento19/ 20 portabilidad	
Sección 4. Derecho oposición y decisiones individuales automatizadas Art. 21 derecho oposición	
Art. 22 decisiones individuales automatizadas, incluida elaboración perfiles	Título IV. Disposiciones aplicables a tratamientos concretos. Art.19 tratamiento datos contactos empresarios individuales/ art.20 sistemas información crediticia/ art.21 Tratamiento relacionados determinadas operaciones mercantiles/ art.22 tratamientos con fines videovigilancia/art.23 Sistemas exclusión publicitaria/ art.24 información denuncias internas/ art.25 tratamiento datos en ámbito función estadística pública/ art.26 fines archivo interés público por AAPP/

	art.27Tratamiento de datos relativos a infracciones y sanciones administrativas
Sección 5. Limitaciones Art. 23 limitaciones	
CAP.IV Responsable de tratamiento y encargado de tratamiento	Titulo V. Responsable y encargado de tratamiento
Sección.1 obligaciones generales	Cap. I. Disp. Generales. Medidas responsabilidad activa
Art24. Responsabilidad del responsable del tratamiento	Art.28 Obligaciones generales del responsable y encargado del tratamiento
Art.25 protección de datos desde el diseño y por defecto	
Art. 26 Corresponsables tratamiento	Art 29 supuestos de corresponsabilidad en el tratamiento
Art.27 Representantes de responsables o encargados del tratamiento no establecidos en la Unión	Art.30. Representantes de los responsables o encargados del tratamiento no establecidos en la UE.
Art.28 Encargado del tratamiento	Cap. II. Encargado tratamiento art.33
Art 29 Tratamiento bajo la autoridad del responsable o del encargado del tratamiento	
Art30. Registro de actividades de tratamiento	Art31. Registro de actividades de tratamiento
Art31. Cooperación con la autoridad de control	Art. 32 Bloqueo datos
Sección 2. Seguridad de los datos personales	
Art.32 Seguridad del tratamiento	
Art33. Notificación de una violación de la seguridad de los datos personales a la autoridad de control	

Art.34 comunicación de una violación de la seguridad de los datos personales al interesado	
Sección3. Evaluación de impacto relativa a la protección de datos y consulta previa Art.35 EVI (evaluación de impacto)	
Art36. Consulta previa	
Sección 4. Delegado protección de datos. Art.37 Designación protección de datos/ art.38 posición delegado de protección de datos/art.39 Funciones del delegado de protección de datos/	Cap. III. DPD Art.34 designación/ art.35 cualificación del delegado/art.36 Posición del delegado de protección de datos/art.37intervención del delegado de protección de datos en caso de reclamación ante las autoridades de protección de datos
Sección5. Códigos conducta y certificación. Art. 40 Códigos de conducta Art41. Supervisión de códigos conducta aprobados Art.42 Certificación Art.43 organismo certificación	Cap. IV. Códigos de conducta y certificación Art.38 Códigos de conducta y art.39 Acreditación de instituciones de certificación
Capítulo V. Transferencias de datos personales a terceros países u organizaciones internacionales Art44. Principio general de transferencias Art.45 Transferencias basada en una decisión de adecuación Art.46 Transferencias mediante garantías adecuadas. Art.47 Normas corporativas vinculantes Art.48 Transferencias o comunicaciones no autorizadas por el derecho de la Unión	Titulo VI. Transferencias internacionales de datos Art.40 Régimen de transferencias internacionales de datos Art.41 Supuestos de adopción por la AEPD Art 42 Supuestos sometidos autorización previa de las autoridades de protección de datos Art.43 supuestos sometidos a información previa a la autoridad de protección de datos competente

Art.49 Excepciones para situaciones específicas Art.50 Cooperación internacional en el ámbito de la protección de datos personales	
Capítulo VI. Autoridades de control independientes Sección 1 independencia Art.51 Autoridad control y 52 independencia Art 53 Condiciones generales aplicable a los miembros de la autoridad de control Art.54 Normas relativas al establecimiento de la autoridad de control	Título VII. Autoridades de protección de datos Cap. I. La agencia española protección de datos. Art.44.Disposiciones generales Art.45 Régimen jurídico Art.46 Régimen económico presupuestario y de personal Art.47 Funciones y potestades de la Agencia Española de Protección de datos Art.48 La presidencia de la AEPD Art.49 Consejo consultivo de la AEPD Art.50 Publicidad
Sección2. Competencia, funciones y poderes Capítulo VII cooperación y coherencia Sección1. Art60. Cooperación entre la autoridad de control principal y las demás autoridades	Sección 2 potestades de investigación y planes de auditorías preventiva Art. 51 Ar52 Art 53 Art 54 Sección 3. Otras potestades de regulación circulares de la AEPD Art.55 Art.56 acción exterior
Art61 Asistencia Mutua	Cap. II. Autoridades autonómicas de protección datos Sección1.
Art.62 operaciones conjuntas de las autoridades de control	Sección2. Coordinación en marco de los procedimientos establecidos en el RGPD

	Tít. VIII. Procedimiento en caso de posible vulneración de la normativa de protección de datos
	Tít. IX Régimen sancionador
	Tít. X Garantías de derechos digitales.

VII. CATÁLOGO DE DERECHOS.

Este catálogo de derechos hace referencia a los derechos reconocidos por el RGPD y la LOPDGDD respecto de los interesados sobre el tratamiento de sus datos, estos vienen recogidos por:

RGPD	LOPDGDD
CAPÍTULO III - Derechos del interesado	TÍTULO III. Derechos de las personas
Sección 1. Transparencia y modalidades	CAPÍTULO I. Transparencia e información
Artículo 12. Transparencia de la información, comunicación y modalidades de ejercicio de los derechos del interesado	Artículo 11. Transparencia e información al afectado.
Sección 2. Información y acceso a los datos personales	Artículo 12. Disposiciones generales sobre ejercicio de los derechos.
Artículo 13. Información que deberá facilitarse cuando los datos personales se obtengan del interesado.	Artículo 13. Derecho de acceso.
Artículo 14. Información que deberá facilitarse cuando los datos personales no se hayan obtenido del interesado.	
Sección 3. Rectificación y supresión	
Artículo 16. Derecho de rectificación.	Artículo 14. Derecho de rectificación.
Artículo 17. Derecho de supresión («el derecho al olvido»).	Artículo 15. Derecho de supresión.
Artículo 18. Derecho a la limitación del tratamiento.	Artículo 16. Derecho a la limitación del tratamiento.
Artículo 19. Obligación de notificación relativa a la rectificación o supresión de datos personales o la limitación del tratamiento.	
Artículo 20. Derecho a la portabilidad de los datos.	Artículo 17. Derecho a la portabilidad.
Sección 4. Derecho de oposición y decisiones individuales automatizadas	
Artículo 21. Derecho de oposición.	Artículo 18. Derecho de oposición.
Artículo 22. Decisiones individuales automatizadas, incluida la elaboración de perfiles.	

Disposiciones generales: La ley orgánica establece que el ejercicio de los derechos que se reconocen se podrá ejercer a través de representantes legal o voluntario. Serán gratuitas las actuaciones llevadas a cabo por el responsable del tratamiento para atender las solicitudes de ejercicio de estos derechos.

En cualquier caso, los titulares de la patria potestad podrán ejercitar en nombre y representación de los menores de catorce años los derechos de acceso, rectificación, cancelación, oposición o cualesquiera otros que pudieran corresponderles en el contexto de la presente ley orgánica.

a) Derecho de acceso

- ✓ El derecho de acceso regulado por la LOPDGDD en su artículo 13 nos remite al art 15 del RGPD el cual establece
- ✓ 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

El interesado tendrá derecho a obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que le conciernen y, en tal caso, derecho de acceso a los datos personales y a la siguiente información:

a) los fines del tratamiento; a conocer el fin al que se va a destinar el tratamiento, es decir para qué se va a utilizar esos datos,

b) las categorías de datos personales de que se trate; a saber, que datos son los que se van a tratar o ser objeto de tratamiento

c) los destinatarios o las categorías de destinatarios a los que se comunicaron o serán comunicados los datos personales, en particular destinatarios en terceros u organizaciones internacionales; a conocer a quienes se les va a trasladar esos tratamientos, sobre todo en el caso de cesión de datos a terceros a conocer la legitimación de esa cesión

d) de ser posible, el plazo previsto de conservación de los datos personales o, de no ser posible, los criterios utilizados para determinar este plazo; a conocer qué plazo esos datos van a conservarse y si no se puede especificar hacer conocedor al interesado de qué criterios se utilizan para determinar este plazo.

Por ejemplo: en el caso de la realización de facturas un plazo de conservación lógico de esos datos sería el necesario para cumplir con las obligaciones tributarias 4 años, no se establece un periodo concreto y se deberá acudir a la normativa específica.

En el blog de protección de datos para empresas y autónomos[52] se relaciona la siguiente lista a modo de ejemplo y hacernos una idea más clara de cuáles pueden ser esos periodos.

- Ley General de Telecomunicaciones
  Se establece un periodo de prescripción de sanciones de:
- muy graves a los **3 años**
- las graves a los **2 años**
- leves a los **6 meses**.

- Código de comercio

En una sociedad, existe una serie de documentación que se deberá conservar al menos durante **6 años**:

- Libro diario
- Registro de inventarios y balances
- Facturas emitidas
- Facturas recibidas

- Reglamento de facturación

Esta normativa enuncia que en el caso de que sea una **persona física** el emisor o receptor, el período de conservación de la **factura** será de **5 años** a partir de su emisión.

Las facturas en las que el emisor o receptor sea persona física, se deben conservar durante un período de cinco años a partir de su emisión.

- Ley General Tributaria

Esta normativa dispone un plazo de **4 años** para que se puedan ejercitar derechos, ya sean formales o económicos por parte del contribuyente o la Administración.

Por lo tanto, almacena el IVA y el IRPF durante 4 años por si acaso.

- Ley de Prevención de Blanqueo de Capitales15

Los sujetos obligados conservarán durante un período mínimo de **10 años** la documentación en que se formalice el cumplimiento de las obligaciones establecidas en dicha Ley.

[52] https://protecciondatoslopd.com/empresas/conservarciondatosplazo/#Ley_Organica_de_Proteccion_de_Datos,consulta 14/04/2019

- Seguridad Social

Queda establecido que para que prescriba la obligación del pago de las **cuotas** a la Seguridad Social han de pasar **5 años**, contar desde la fecha en la que debieron ser ingresadas.

Documentación relativa a los expedientes generados por un abogado o procurador

Se deben conservar al menos durante **5 años** los expedientes ya que es el plazo en el cual se podrán ejercitar responsabilidades profesionales.

- Ley de mediación en asuntos civiles y mercantiles

Como es lógico, un procedimiento de mediación puede concluir con acuerdo o no, y sobre el mismo pueden recaer futuras responsabilidades.

Por lo tanto, se almacenará al menos durante **4 meses** el expediente de la mediación.

- Videovigilancia

Las imágenes/sonidos captados por los sistemas de videovigilancia **serán cancelados** en el plazo máximo de **1 mes** desde su captación.

Excepciones

Si de la observación de las grabaciones se aprecian infracciones penales o administrativas graves o muy graves y existe una investigación policial en curso **no** se podrán eliminar.

Acceso a edificios

1 mes para cancelar los datos incluidos en ficheros automatizados para controlar el acceso a edificios.

- Ley de Seguridad Privada

Los informes de investigación deberán conservarse archivados, al menos, durante **3 años,** incluidas las imágenes grabadas.

No obstante, lo datos estarán **debidamente bloqueados.**

- Ley Reguladora de la Autonomía del Paciente

Como regla general se puede almacenar durante **5 años** la **documentación clínica**, a contar desde la fecha en la que se da de alta al paciente.

Casos especiales

No obstante, en algunas comunidades autónomas, para ciertos casos se prevé un periodo diferente de conservación.

Ley 7/2002 de 10 diciembre CA Cantabria, ordenación sanitaria

15 años para la conservación de la historia clínica desde la muerte del paciente.

- Ley 3/2001, de 28 mayo CA Galicia, consentimiento informado e historia clínica de los pacientes

- Se conservarán de forma **indefinida:**
- informes de alta
- hojas de consentimiento informado
- hojas de alta voluntaria
- informes quirúrgicos y/o registros de parto
- documentos de anestesia
- informes de exploraciones complementarias. Documentación relativa a necropsias
- hoja de evolución y de planificación de cuidados de enfermería
- otros informes médicos
- cualquier otra información que se considere relevante a efectos asistenciales, preventivos, epidemiológicos o de investigación
- información de aquellas historias clínicas cuya conservación sea procedente por razones judiciales

- Ley 178/2005 de 26 jul. CA Canarias que regula la historia clínica en los centros y establecimientos hospitalarios

- Se conservarán durante **20 años** desde la última acción asistencial la siguiente documentación:
- autorización de ingreso
- consentimiento informado
- hoja quirúrgica
- órdenes médicas
- informe de control de medicación
- hojas del recién nacido, de su propia historia clínica
- informes de anestesia
- listas transfusión
- informes de exploraciones complementarias
- solicitud de alta voluntaria
- informes de Anatomía Patológica.
- documentación de necropsias.
- información de aquellas historias clínicas cuya conservación sea procedente por razones judiciales
- No obstante, se conservarán de manera **definitiva:**
- los informes clínicos de alta
- las hojas de anamnesis y exploración física y las hojas de evolución de los episodios asistenciales de los que no exista informe de alta

- Decreto 38/2012, de 13 de marzo, País Vasco, sobre historia clínica y derechos y obligaciones de pacientes y profesionales de la salud en materia de documentación clínica

Se podrá destruir toda la documentación clínica de un paciente una vez transcurridos **10 años** desde su fallecimiento.

También se podrá destruir la histórica clínica que haya permanecido sin movimientos durante **15 años.**

Reglamento de centros de reconocimiento destinados a verificar las aptitudes psicofísicas de los conductores

El centro conservará durante **10 años** el contenido de los informes emitidos, así como los documentos que aportó, en su momento el interesado.

Derecho hotelero

- Los libros-registro de entrada en los establecimientos hoteleros deberán almacenarse durante **3 años,** a disposición de los Cuerpos y Fuerzas de Seguridad del Estado.

Derecho de Internet

- Los prestadores de servicios de comunicaciones electrónicas podrán conservar al menos durante **1 año**:
- ✓ Identificador de usuario
- ✓ dirección IP
- ✓ número de teléfono
- ✓ IMSI e IMEI
- ✓ fecha y hora de la comunicación electrónica
- ✓ identificación del tipo de servicio utilizado (voz, datos, SMS o MMS)

e) la existencia del derecho a solicitar del responsable la rectificación o supresión de datos personales o la limitación del tratamiento de datos personales relativos al interesado, o a oponerse a dicho tratamiento; esto quiere decir que el interesado en cualquier momento puede solicitar al responsable la rectificación o supresión de datos personales o la limitación de estos, salvo que no puedan ser suprimidos por el cumplimiento de las obligaciones legales anteriormente expuestas.

f) el derecho a presentar una reclamación ante una autoridad de control; es decir cuando un interesado entienda que sus datos han sido tratados vulnerando alguno de los anteriores preceptos o sus peticiones no son atendidas por razones no fundadas en obligaciones legales, podrán interponer una denuncia en la agencia de control, es decir Agencia Española de Protección de Datos. No obstante, entre la Agencia de control y el usuario, podrá aparecer la figura de delegado de protección de datos anteriormente descrito que realizará las funciones de intermediador entre la Agencia y el interesado.

g) cuando los datos personales no se hayan obtenido del interesado, cualquier información disponible sobre su origen; esto indica que, si el interesado no ha proporcionado los datos directamente al responsable o persona que está tratando los datos, este tiene derecho a conocer cómo se han obtenidos los datos.

h) la existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22RGPD, apartados 1 y 4, 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.

1.Todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar.

2. 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 en virtud del artículo 46 relativas a la transferencia.

3. El responsable del tratamiento facilitará una copia de los datos personales objeto de tratamiento. El responsable podrá percibir por cualquier otra copia solicitada por el interesado un canon razonable basado en los costes administrativos. Cuando el interesado presente la solicitud por medios electrónicos, y a menos que este solicite que se facilite de otro modo, la información se facilitará en un formato electrónico de uso común. En este caso se establece que el responsable facilitará copia de los datos en formato portable preferiblemente en medio electrónico, pero esto no es obligatorio ya que permite la posibilidad de solicitar de que se facilite de otro modo. (hacer alusión a la 39/2015 comunicación administración e interesado)

4. El derecho a obtener copia mencionado en el apartado 3 no afectará negativamente a los derechos y libertades de otros.

En la AEPD nos indican cómo podemos solicitar esos datos:

- 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

El formulario de petición de datos y para ejercitar el derecho de acceso a estos es el siguiente:

https://www.aepd.es/media/formularios/formulario-derecho-de-acceso.pdf

Pongamos, por ejemplo: conocemos que la compañía ORANGE está haciendo uso de mis datos con fines comerciales y queremos conocer que datos son los que obran en su poder. Podremos buscar en su página web la cuenta de correo electrónico del DPD y remitirle dicha solicitud. Dicha información suele estar en la parte de política de privacidad de la empresa. En el caso práctico sería esta la información:

orangeproteccion.datos@orange.com

b) Derecho de rectificación

El ejercicio de este derecho supone que podrás obtener la rectificación de tus datos personales que sean inexactos sin dilación indebida del responsable del tratamiento[53].

Teniendo en cuenta los fines del tratamiento, tienes derecho a que se completen los datos personales que sean incompletos, inclusive mediante una declaración adicional.

En tu solicitud deberás indicar a qué datos te refieres y la corrección que hay que realizar. Además, cuando sea necesario, deberás acompañar tu solicitud de la documentación que justifique la inexactitud o el carácter incompleto de tus datos.

Este es el formulario que se propone https://www.aepd.es/media/formularios/formulario-derecho-de-rectificacion.pdf

c) Derecho de oposición

Este derecho, como su nombre indica, supone que te puedes oponer a que el responsable realice un tratamiento de los datos personales en los siguientes supuestos:

Cuando sean objeto de tratamiento basado en una misión de interés público o en el interés legítimo, incluido la elaboración de perfiles:

El responsable dejará de tratar los datos salvo que acredite motivos imperiosos que prevalezcan sobre los intereses, derechos y libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones

Cuando el tratamiento tenga como finalidad la mercadotecnia directa, incluida también la elaboración de perfiles anteriormente citada:

Ejercitado este derecho para esta finalidad, los datos personales dejarán de ser tratados para dichos fines

Este es el enlace del formulario proporcionado por la AEPD: https://www.aepd.es/media/formularios/formulario-derecho-de-oposicion.pdf

[53] https://www.aepd.es/reglamento/derechos/index.html, consulta 14/04/2019

- ❖ Un caso que supuso una especial polémica fue el tratamiento de datos por parte de los partidos políticos, concretamente el art. 58 bis, la cesión de los datos a estos y su tratamiento posterior, supuso que se elevara al Tribunal constitucional un recurso inconstitucionalidad respecto a este. l Pleno del Tribunal Constitucional por unanimidad ha declarado inconstitucional el artículo 58 bis 1 de la Ley Electoral General. Dicho artículo permitía a los partidos recopilar datos relativos a las opiniones políticas de los ciudadanos. Estima así el recurso presentado por el Defensor del pueblo. El tribunal considera que la Disposición Final Tercera de la Ley Orgánica de Protección de Datos (LOPDGDD), que añade un nuevo artículo 58 bis a la Ley Orgánica de Régimen Electoral General (LOREG), vulnera derechos fundamentales de la Constitución.

La sentencia señala que *"el legislador no ha precisado qué finalidad o bien constitucional justifica la restricción del derecho a la protección de datos personales ni ha determinado en qué supuestos y condiciones puede limitarse, mediante reglas precisas que hagan previsible al interesado la imposición de tal limitación y sus consecuencias".*

Respecto a este pronunciamiento y el derecho a oposición se posibilitó por parte de la administración que se pudiera ejercer dicho derecho de oposición respecto procesos electorales, es novedoso y numerosos ciudadanos ya han ejercicio de "supresión", realmente lo que se evita es que se traslade los datos a los partidos políticos para el envío de información y propaganda electoral.

Este procedimiento permite la cumplimentación vía web de la solicitud de exclusión/inclusión en las copias del censo electoral que se entregan a los representantes de las candidaturas para realizar envíos postales de propaganda electoral.

- ✓ Las exclusiones solicitadas hasta el día decimotercero posterior a la convocatoria de un proceso electoral tendrán efectos en dicho proceso y en todos los posteriores, en tanto no se manifieste lo contrario por el elector. Se podrán realizar aquí en el instituto nacional de estadística: https://sede.ine.gob.es/oposicionPartidos (actualmente inactivo).

d) Derecho de supresión ("al olvido")

En un primer momento debemos considerar que el derecho de supresión, regulado por los artículos 17 del RGPD y el 15 del LOPDGDD y el derecho de olvido en búsquedas de internet, regulado por los artículos 93 y 94 de la LOPDGDD son dos modalidades distintas de ejercicio del derecho de supresión. Mientras que los primeros serían de los ficheros y bases de datos objeto de tratamiento, los segundos se refieren a aquellos datos que estén dentro de los motores de búsqueda (Google) y frente a los servicios de redes sociales y servicios de la sociedad de la información equivalentes.

Podrás ejercitar este derecho ante el responsable solicitando la supresión de sus datos de carácter personal cuando concurra alguna de las siguientes circunstancias:

- Si tus datos personales ya no son necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo
- Si el tratamiento de tus datos personales se ha basado en el consentimiento que prestaste al responsable, y retiras el mismo, siempre que el citado tratamiento no se base en otra causa que lo legitime
- Si te has opuesto al tratamiento de tus datos personales al ejercitar el derecho de oposición en las siguientes circunstancias

El tratamiento del responsable se fundamentaba en el interés legítimo o en el cumplimiento de una misión de interés público, y no han prevalecido otros motivos para legitimar el tratamiento de tus datos

A que tus datos personales sean objeto de mercadotecnia directa, incluyendo la elaboración perfiles relacionada con la citada mercadotecnia

- Si tus datos personales han sido tratados ilícitamente
- Si tus 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
- Si los datos personales se han obtenido en relación con la oferta de servicios de la sociedad de la información mencionados en el artículo 8, apartado 1 (condiciones aplicables al tratamiento de datos de los menores en relación con los servicios de la sociedad de la información).

No obstante, este derecho no es ilimitado, de tal forma que puede ser factible no proceder a la supresión cuando el tratamiento sea necesario para el ejercicio de la libertad de expresión e información, para el cumplimiento de una obligación legal, 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 de interés público, fines de investigación científica o histórica o fines estadísticos, o para la formulación, el ejercicio o la defensa de reclamaciones.

Formulario de AEPD; https://www.aepd.es/media/formularios/formulario-derecho-de-supresion.pdf

Por otro lado, Google ha habilitado un formulario online por el cual se puede realizar esta petición de supresión de datos de los buscadores de internet de esta empresa y aquí están los enlaces:

[54]https://www.google.com/webmasters/tools/legal-removal-request?complaint_type=rtbf&visit_id=636908020850650508-67773449&rd=1

YOUTUBE:

[55]https://www.youtube.com/reportingtool/legal

e) Derecho a la limitación del tratamiento

Este nuevo derecho consiste en que obtengas la limitación del tratamiento de tus datos que realiza el responsable, si bien su ejercicio presenta dos vertientes:

Puedes solicitar la suspensión del tratamiento de tus datos:

Cuando impugnes la exactitud de tus datos personales, durante un plazo que permita al responsable su verificación

Cuando te hayas opuesto al tratamiento de tus datos personales que el responsable realiza en base al interés legítimo o misión de interés público, mientras aquel verifica si estos motivos prevalecen sobre los tuyos

Solicitar al responsable la conservación tus datos:

Cuando el tratamiento sea ilícito y te has opuesto a la supresión de tus datos y en su lugar solicitas la limitación de su uso

Cuando el responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones

[54]https://www.google.com/webmasters/tools/legalremovalrequest?complaint_type=rtbf&visit_id=636908020850650508-67773449&rd=1, fecha de consulta 14/04/2019
[55] https://www.youtube.com/reportingtool/legal, consulta 14/04/2019

Formulario de ejercicio del derecho de limitación proporcionado por la AEPD:

https://www.aepd.es/media/formularios/formulario-derecho-de-limitacion.pdf

f) Derecho a la portabilidad

La finalidad de este nuevo derecho es reforzar aún más el control de tus datos personales, de forma que cuando el tratamiento se efectúe por medios automatizados, recibas tus datos personales en un formato estructurado, de uso común, de lectura mecánica e interoperable, y puedas transmitirlos a otro responsable del tratamiento, siempre que el tratamiento se legitime en base al consentimiento o en el marco de la ejecución de un contrato.

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.

Formulario de ejercicio del derecho de limitación proporcionado por la AEPD:

https://www.aepd.es/media/formularios/formulario-derecho-de-portabilidad.pdf

g) Derecho a no ser objeto de decisiones individuales automatizadas

Este derecho pretende garantizar que no seas objeto de una decisión basada únicamente en el tratamiento de tus datos, incluida la elaboración de perfiles, que produzca efectos jurídicos sobre ti o te afecte significativamente de forma similar.

Sobre esta elaboración de perfiles, se trata de cualquier forma de tratamiento de tus datos personales que evalúe aspectos personales, en particular analizar o predecir aspectos relacionados con tu rendimiento en el trabajo, situación económica, salud, las preferencias o intereses personales, fiabilidad o el comportamiento.

No obstante, este derecho no será aplicable cuando:

Sea necesario para la celebración o ejecución de un contrato entre tú y el responsable

El tratamiento de tus datos se fundamente en tu consentimiento prestado previamente

No obstante, en estos dos primeros supuestos, el responsable deber garantizar tu derecho a obtener la intervención humana, expresar tu punto de vista e impugnar la decisión.

Esté autorizado por el Derecho de la Unión o de los Estados miembros y se establezcan medidas adecuadas para salvaguardar los derechos y libertades e intereses legítimos del interesado.

A su vez, estas excepciones no se aplicarán sobre las categorías especiales de datos (art.9.1), salvo que se aplique el artículo 9.2. letra a) o g) y se hayan tomado las medidas adecuadas citadas en el párrafo anterior.

h) Derecho de información

Cuando se recaban tus datos de carácter personal, el responsable del tratamiento debe cumplir con el derecho de información. Para dar cumplimiento a este derecho, la AEPD recomienda que esta información se te facilite por capas o niveles de manera que:

Se te facilite una información básica en un primer nivel, de forma resumida, en el mismo momento y en el mismo medio en que se recojan tus datos personales.

Y, por otra parte, que se te remita el resto de las informaciones, en un medio más adecuado para su presentación, compresión y, si se desea, archivo.

La información a facilitar por capas o niveles sería la siguiente:

1.ª Capa: Información básica (resumida)

La identidad del responsable del tratamiento

Una descripción sencilla de los fines del tratamiento, incluyendo la elaboración de perfiles si existiese

La base jurídica del tratamiento

Previsión o no de cesiones. Previsión o no de transferencias a terceros países

Referencia al ejercicio de derechos

2.ªCapa: Información adicional (detallada)

Datos de contacto del responsable. Identidad y datos del representante (si existiese). Datos de contacto del delegado de protección de datos (si existiese).

Descripción ampliada de los fines del tratamiento. Plazos o criterios de conservación de los datos. Decisiones automatizadas, perfiles y lógica aplicada.

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 o categorías de destinatarios. Decisiones de adecuación, garantías, normas corporativas vinculantes o situaciones específicas aplicables.

Cómo ejercer los derechos de acceso, rectificación, supresión y portabilidad de los datos, y la limitación u oposición a su tratamiento. Derecho a retirar el consentimiento prestado. Derecho a reclamar ante la Autoridad de Control.

Datos no obtenidos directamente de ti

En el supuesto en que tus datos personales no hayan sido obtenidos directamente de ti, se te facilitará, además de la información indicada anteriormente:

- En la información básica (1ª capa, resumida):la fuente (procedencia) de los datos
- Y en la información adicional (2ª capa, detallada):la información detallada del origen de los datos, incluso si proceden de fuentes de acceso público la categoría de datos que se traten.

Esta información se te facilitará dentro de un plazo razonable, y más tardar en un mes, salvo que:

Si los datos personales han de utilizarse para una comunicación con el afectado, a más tardar en el momento de la primera comunicación a dicho afectado

Si está previsto comunicarlos a otro interesado, a más tardar en el momento en que los datos personales sean comunicados por primera vez.

Un ejemplo de esta información de primera capa podría ser la siguiente:

INFORMACIÓN BÁSICA DE PROTECCIÓN DE DATOS

RESPONSABLE: TU ELECTRODOMESTICO S.L

FINALIDAD: prestar servicio, podría incluir alguna comunicación posterior para realizar un seguimiento y encuesta de satisfacción por la compra.

LEGITIMACIÓN: ejecución del contrato de servicio, además del interés legítimo del responsable según se desprende del considerando 47 RGPD

DESTINATARIOS: los datos proporcionados solo serán cedidos al fabricante para activar la garantía de la misma. Por lo que puede suponer la cesión a terceros países ya que algunos de los productos suministrados por el responsable son fabricados en países no pertenecientes a la Unión Europea, no obstante, dicha cesión solo se realizará para cumplir con la garantía del producto suministrado. Los terceros países son los siguientes:

Le informamos que los datos serán transferidos a una entidad ubicada en ARGENTINA, país que garantiza un nivel de protección adecuado, según decisión de la Comisión.

Le informamos que los datos serán transferidos a una entidad en ECUADOR con la que se ha establecido un contrato que incluye las cláusulas tipo de protección de datos adoptadas por la Comisión y que puede consultarse en www.OLX.com/tid

DERECHOS: se podrán ejercer derechos de acceso, rectificación y supresión de datos, tal y como se explica en la información adicional, (ARCO).

INFORMACIÓN ADICIONAL: puede consultar la información detallada de protección de datos en WWW.TU ELECTRODOMESTICO S.L /protecciónde datos

En esta página y en el epígrafe de tratamiento de datos se relacionarán los derechos con más profundidad:

- Derecho a solicitar el acceso a los datos personales relativos al interesado,
- Derecho a solicitar su rectificación o supresión,
- Derecho a solicitar la limitación de su tratamiento,
- Derecho a oponerse al tratamiento
- Derecho a la portabilidad de los datos

DPO: Se podrá ejercer los derechos a través de la cuenta de correo

protecciónde datos@dpotuelectrodoméstico.es o si esa gestión ha sido encomendada a mi persona como gestora de datos vlrodpo@hotmail.es

VIII. NUEVOS DERECHOS DIGITALES

La nueva LOPDGDD trae consigo a su vez un catálogo de nuevos derechos digitales, estos son los contemplados en el título X del art. 79 al 97. Hay que destacar que dentro de estos derechos digitales se debe dividir en dos grupos a su vez, ¿por qué? Bien pues porque hay una parte del catálogos de derechos para los cuales no es de aplicación el RGP y tampoco la LOPDGDD en cuanto al procedimiento de reclamación de incumplimiento de estos y son los que van del art. 79 al 88 y los que van del 95 al 97, esos derechos estarían fuera del ámbito de aplicación de protección de datos desde el punto de vista de protección y es que se deberá determinar quién es el órgano competente y la vía jurisdiccional oportuna para poder reclamar, abarcando del 89 al 94 los artículos que sí se les aplicaría la normativa de protección de datos[56].

Ejemplo: El derecho de desconexión digital no se cumpliese se deberá acudir a la autoridad laboral competente. Sin embargo, hay que destacar que quizás la capacidad de protección de este derecho quede muy limitada sobre todo porque no se ha incluido en la legislación modificación alguna en Real Decreto Legislativo 5/2000, de 4 de agosto, por el que se aprueba el texto refundido de la Ley sobre Infracciones y Sanciones en el Orden Social.[57]

O por ejemplo en ejercicio del derecho del testamento digital deberíamos acudir a vía civil.

Vamos a repasar los derechos digitales y destacaremos con más intensidad alguno de ellos:

Educación digital. Art.83 en concurrencia con la DA21 de la ley.

Será obligatoria la educación digital y se da un plazo de 1 año para implantar esta asignatura, no solo en el ámbito de educación básica sino en la universitaria, implantándolo como asignatura y modificando la ley de universidades añadiéndolo como derecho.

Además, las Administraciones Públicas incorporarán a los temarios de las pruebas de acceso a los "cuerpos superiores y a aquéllos en que habitualmente se desempeñen funciones que impliquen el acceso a datos personales materias relacionadas con la garantía de los derechos digitales y en particular el de protección de datos".

[56] "marco legislativo local y nacional" Curso protección de datos INAP, a funcionarios de las AAPP Locales, epígrafe Derechos Digitales. 25/10/2019.

[57] https://www.boe.es/eli/es/rdlg/2000/08/04/5/con Real Decreto Legislativo 5/2000, de 4 de agosto, por el que se aprueba el texto refundido de la Ley sobre Infracciones y Sanciones en el Orden Social.

Pese a estar fuera de los contemplados dentro del ámbito de protección de datos, las autoridades de control han solicitado la inclusión de este derecho además de realizar campañas de concienciación del uso de dispositivos digitales y educativas sobre el buen uso de las TICs[58]

Derecho protección de los menores en internet.art.84

1. Los padres, madres, tutores, curadores o representantes legales procurarán que los menores de edad hagan un uso equilibrado y responsable de los dispositivos digitales y de los servicios de la sociedad de la información a fin de garantizar el adecuado desarrollo de su personalidad y preservar su dignidad y sus derechos fundamentales.

2. La utilización o difusión de imágenes o información personal de menores en las redes sociales y servicios de la sociedad de la información equivalentes que puedan implicar una intromisión ilegítima en sus derechos fundamentales determinará la intervención del Ministerio Fiscal, que instará las medidas cautelares y de protección previstas en la Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor.

[58] https://ecodiario.eleconomista.es/espana/noticias/7638101/06/16/Clan-y-la-AEPD-lanzan-una-campana-de-educacion-digital-para-fomentar-el-buen-uso-de-Internet-y-las-redes-sociales.html

La AEPD junto con la fundación ANAR realizaron un decálogo de garantías y derechos de los menores en relación con las tecnologías. [59]

También se han habilitado páginas web que orientan como realizar un uso responsable de las TICs en menore como la https://www.is4k.es (Instituto seguridad de España for kids, para niños) o teléfonos de atención gratuito como el de la Comunidad Valenciana 900116117.

I. Sobre el interés superior del menor

Debe primar el interés superior del menor también en el entorno digital. Cualquier servicio de la sociedad de la información o dispositivo tecnológico dirigido a niños/as o adolescentes, o susceptible de ser usado por ellos, garantizará la protección del interés superior del menor y de sus derechos fundamentales.

II. Sobre el derecho a la salud y a la seguridad Protección frente a los contenidos y dispositivos.

Los menores de edad tienen derecho a un entorno digital en el que estén protegidos frente a cualquier tipo de violencia o abuso realizado a través o mediante la tecnología.

III. Sobre el derecho a la intimidad y a su imagen Asegurar la privacidad.

Los menores tienen derecho al honor, a la intimidad y a la propia imagen. Este derecho comprende también el secreto de sus comunicaciones digitales.

(Se realiza desarrollo a respecto de este derecho en el epígrafe de supuestos prácticos, ya que genera un conflicto con el deber de cuidados de los padres o tutores respecto de sus hijos y la responsabilidad de estos respecto de los menores)

IV. Sobre el derecho a la protección de datos personales y el derecho al olvido en redes sociales

Proteger sus datos personales y garantizar que puedan borrar su historial digital.

Estos derechos incluyen que deba contarse con su consentimiento, si es mayor de 14 años, o el de sus representantes legales, para la publicación o difusión de sus datos personales o su imagen a través de servicios de redes sociales o servicios equivalentes.

Igualmente incluye el derecho al olvido en búsquedas de Internet y en redes sociales, facilitándoles que puedan borrar su 'huella digital' (su historial en Internet) cuando así lo consideren.

[59] https://www.aepd.es/prensa/2019-07-29-aepd-anar-mar-espana-carta-derechos-ninos-adolescentes.html

V. Sobre el derecho al acceso a Internet

Acceso debidamente protegido. Los menores de edad tienen derecho a acceder a Internet y a las tecnologías de la información sin ningún tipo de discriminación por razón de renta familiar, zona geográfica, discapacidad o cualquier otro motivo.

Al mismo tiempo, este acceso a las tecnologías debe estar tutelado por sus padres, tutores o representantes legales asegurando que los contenidos y dispositivos a los que va a acceder no son perjudiciales ni para él ni para otros.

VI. Sobre el Derecho a la información y a la educación

Velar por una información veraz y responsable. Los menores de edad tienen derecho a acceder a la información y a la educación a través de Internet y medios tecnológicos.

VII. Sobre el derecho a ser oídos y escuchados

Líneas de Ayuda a la Infancia. Los menores de edad tienen reconocido el derecho a ser escuchados a través de las Líneas de Ayuda a la Infancia (en España Teléfono y Chat ANAR) para que cualquier niño/a en riesgo conozca que existe este recurso y acceda al mismo siempre que lo necesite.

VIII. Sobre el derecho de participación

Participar en los asuntos que les afecten. Los menores de edad tienen derecho a participar y expresar su opinión en los asuntos que les afectan. Se potenciará el uso de las tecnologías para el pleno desarrollo de este derecho.

Este derecho incluye el derecho a la libertad de asociación y de celebrar reuniones con fines pacíficos en el entorno digital9.

IX. Sobre el derecho a la libertad de expresión

Libertad de expresión y opinión. Los menores de edad tienen derecho a expresar libremente sus opiniones e ideas a través de medios tecnológicos, con los únicos límites que marcan los estándares internacionales para el respeto de los derechos y la reputación de los demás.

X. Sobre el derecho al ocio, al juego y a la cultura

Derecho al esparcimiento y a la cultura. Los menores de edad tienen derecho al esparcimiento, al juego y a las actividades recreativas propias de su edad, también a través de medios tecnológicos, sin olvidar que el juego de forma

presencial y con interacción real con sus iguales es necesario para su adecuado desarrollo psicológico.

Se debe propiciar el acceso de los menores de edad a la cultura y las artes, potenciando las oportunidades de la tecnología para ello.

Art.92 Protección de datos de los menores en internet.

Artículo 92. Protección de datos de los menores en Internet. Los centros educativos y cualesquiera personas físicas o jurídicas que desarrollen actividades en las que participen menores de edad garantizarán la protección del interés superior del menor y sus derechos fundamentales, especialmente el derecho a la protección de datos personales, en la publicación o difusión de sus datos personales a través de servicios de la sociedad de la información. Cuando dicha publicación o difusión fuera a tener lugar a través de servicios de redes sociales o servicios equivalentes deberán contar con el consentimiento del menor o sus representantes legales, conforme a lo prescrito en el artículo 7 de esta ley orgánica.

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

Artículo 87. Derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral.

1. Los trabajadores y los empleados públicos tendrán derecho a la protección de su intimidad en el uso de los dispositivos digitales puestos a su disposición por su empleador.

2. 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.

3. 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.

La sentencia de 8 de febrero de 2018 fija la doctrina del Tribunal Supremo teniendo en cuenta la sentencia del Tribunal Europeo de Derechos Humanos Barbulescu II

"La Sentencia del Tribunal Supremo de 8 de febrero de 2018, dictada en el recurso de casación para la unificación de la doctrina núm. 1121/2015, analiza por primera vez el cumplimiento por parte de una empresa de la doctrina fijada por la Sentencia de la Gran Sala del Tribunal Europeo de Derechos Humanos (TEDH) de 5 de septiembre de 2017, en el caso Barbulescu II, en relación con la posibilidad de revisar los correos electrónicos de un trabajador.

En el supuesto de hecho analizado, la empresa había procedido al despido del trabajador demandante por motivos disciplinarios como consecuencia de un incumplimiento muy grave de su código ético. El incumplimiento, indiciariamente, se detectó a través de un hallazgo casual, que fue corroborado a través de una investigación interna llevada a cabo por la propia compañía, que incluyó la revisión de determinados correos electrónicos del actor. La empresa contaba con una política clara de utilización de los medios informáticos, que establecía tanto la prohibición del uso personal de las herramientas informáticas de trabajo como la posibilidad de que la empresa pudiera vigilar el cumplimiento por parte de sus empleados de tal política. Asimismo, todos los trabajadores de la empresa (incluido el empleado despedido), antes de iniciar una sesión en los sistemas informáticos de la compañía, debían aceptar (a través del correspondiente "clic") un recordatorio de sus políticas de uso, en el que se les reiteraba que solo estaba permitido un uso exclusivamente profesional de los medios informáticos y que la

empresa podía controlar ese uso. La investigación iniciada por la empresa trajo causa del hallazgo casual en una impresora de uso compartido de dos resguardos de transferencias efectuadas por un proveedor de la empresa a favor del demandante. El trabajador interaccionaba habitualmente por razón de su trabajo con el mencionado proveedor y la conducta descrita se encontraba expresamente prohibida por el código ético de la empresa. En lo que ahora interesa, la investigación se limitó a un análisis de aquellos correos electrónicos que podían tener alguna relación con las transferencias localizadas, utilizando para ello limitaciones temporales y palabras clave de búsqueda. La sentencia de instancia y la sentencia del Tribunal Superior de Justicia de Galicia que resolvió el recurso de suplicación presentado por el actor declararon la procedencia del despido, si bien la sentencia de suplicación consideró nula la prueba obtenida por la empresa consistente en la revisión de correos electrónicos, por entender que se había vulnerado el secreto de las comunicaciones del trabajador. La empresa y el trabajador recurrieron en casación para la unificación de la doctrina frente a la sentencia de suplicación. Mientras que el Tribunal Supremo desestimó (por falta de contradicción) el recurso interpuesto por el trabajador, estimó el recurso de la empresa, revocando parcialmente la sentencia de suplicación en lo referente a la validez de la prueba obtenida. El Tribunal Supremo, antes de entrar a analizar en profundidad el recurso de la empresa y la aplicabilidad de la doctrina del TEDH en el caso Barbulescu, analiza y acepta la posibilidad de que una empresa recurra una sentencia, aunque esta contenga un fallo plenamente estimatorio de sus pretensiones.

En concreto, el Tribunal Supremo concluye que no se puede negar el acceso al recurso a la empresa, dado que: (i) estaba en juego la determinación de la extensión de los poderes empresariales de control; (ii) se debe permitir a la empresa acreditar todos los incumplimientos imputados en la carta de despido; y (iii), especialmente, la empresa debe tener la posibilidad de revocar la declaración de que había infringido los derechos fundamentales del actor, lo que podría dar lugar a responsabilidades de toda índole. Del mismo modo, el Tribunal Supremo concluye que la sentencia alegada como contradictoria por la empresa, la Sentencia del Tribunal Constitucional núm. 170/2013, de 7 de octubre, es una sentencia válida a efectos de casación unificadora de doctrina y que, además, es la que contiene la doctrina acertada sobre la materia. Así, el Tribunal Supremo considera que la sentencia de contraste es consecuente con un consolidado cuerpo jurisprudencial emanado del Tribunal Supremo(Sentencias del Tribunal Supremo de 26 de septiembre de 2007, de 8 de marzo de 2011 y de 6 de octubre de 2011) y del propio Tribunal Constitucional, que resume de la siguiente manera: 1) El poder de control empresarial: (a) es indispensable para la buena marcha de la organización productiva; (b) en las relaciones laborales se ha de producir una necesaria coordinación entre el interés y los derechos del trabajador y los de la empresa; y (c) el empresario puede regular el uso de los medios y sistemas informáticos de su titularidad, así como la facultad de su vigilancia y control. 2) El derecho a la intimidad: (a) garantiza el secreto respecto de la vida personal, cuyos contornos no pueden ser delimitados por terceros; (b) no se reduce al ámbito doméstico, sino que incluye otros ámbitos como el del trabajo;

y (c) no es un derecho absoluto, sino que se puede ver limitado por otros fines constitucionalmente legítimos, siempre que sea de forma proporcionada. 3) El correo electrónico facilitado por el empresario puede formar parte del ámbito de protección del derecho a la intimidad, en función de las condiciones e instrucciones de uso fijadas por el propio empresario, ya que ello determinará la expectativa razonable de privacidad y confidencialidad del trabajador. 4) A la hora de llevar a cabo el control empresarial se deberá tener en cuenta: (i) la expectativa de privacidad, inexistente en supuestos de prohibición absoluta de uso personal de los medios empresariales; y (ii) los tradicionales criterios de idoneidad, necesidad y proporcionalidad de la medida de control empleada. El Tribunal Supremo concluye que la conducta empresarial descrita cumple "holgadamente" los criterios expuestos, por lo que no se ha producido una vulneración de los derechos fundamentales del actor. Asimismo, considera que la doctrina fijada por el TEDH en el caso Barbulescu II es sustancialmente coincidente con la jurisprudencia constitucional española, ya que ambas tienen como objetivo cohonestar el derecho a la vida privada y al secreto de las comunicaciones del trabajador con la facultad empresarial de comprobar la actividad profesional de sus trabajadores. En este sentido, el Tribunal Supremo considera que los criterios enunciados en el caso Barbulescu II por el TEDH son perfectamente compatibles y coherentes con los tres principios tradicionales de la doctrina constitucional española (idoneidad, necesidad y proporcionalidad). En concreto, a la hora de realizar el análisis de proporcionalidad tradicionalmente exigido por el Tribunal Constitucional, el Tribunal Supremo afirma que se deberán tener en cuenta los aspectos señalados por el TEDH, es decir: (i) si el empleado fue informado por su empresa de que existían medidas de vigilancia de sus comunicaciones; (ii) cuál fue el alcance de la supervisión realizada y si se limitó a constatar el flujo de comunicaciones o si se accedió también a su contenido; (iii) si existía justificación empresarial para la vigilancia efectuada; (iv) si no existían medios menos intrusivos que los empleados por el empresario para conseguir el objetivo; (v) cuál fue el uso que hizo el empresario de la información obtenida; y (vi) las garantías ofrecidas al empleado, incluida la información previa de la posible revisión. Por tanto, en esta sentencia el Tribunal Supremo ratifica la validez y vigencia de la doctrina y jurisprudencia españolas previas al caso Barbulescu II y ofrece, mediante esta relevante Sentencia, una guía de actuación más clara y precisa a las empresas a la hora de proceder a la revisión del correo electrónico de sus empleados. Autores: Sergio Ponce Rodríguez y Jesús David García Sánchez, socios de Forelab y abogados del despacho Uría y Menéndez[60]

Otra sentencia que viene a reforzar la necesidad de información previa de la empresa sobre los usos de los medios informáticos que esta ponga a disposición del empleador es una de Andalucía

STSJ 28/03/2019 , sobre una empresa que despidió a un empleado por utilizar el ordenador de la empresa para jugar, ver porno e incluso comprar prendas, se

[60] https://elderecho.com/control-por-parte-de-la-empresa-del-correo-electronico-del-empleado

declaró nula la prueba obtenida por el empresario, pues no se cumplió con el deber de informar sobre los usos al empleado, con carácter previo[61].

[61]http://www.poderjudicial.es/search/contenidos.action?action=contentpdf&databasematch=AN&reference=8741724&statsQueryId=120795116&calledfrom=searchresults&optimize=20190425 Sentencia 28/03/2019 Andalucía STSJ

Derecho a la desconexión laboral art. 88

1. 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. 2. 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. 3. El empleador, previa audiencia de los representantes de los trabajadores, elaborará una política interna dirigida a trabajadores, incluidos los que ocupen puestos directivos, en la que definirán las modalidades de ejercicio del derecho a la desconexión y las acciones de formación y de sensibilización del personal sobre un uso razonable de las herramientas tecnológicas que evite el riesgo de fatiga informática. En particular, se preservará el derecho a la desconexión digital en los supuestos de realización total o parcial del trabajo a distancia, así como en el domicilio del empleado vinculado al uso con fines laborales de herramientas tecnológicas.

Se deben establecer claramente los horarios de trabajo efectivo, mediante el uso de políticas internas de la empresa[62].En este sentido, cabe afirmar que los trabajadores tienen derecho a conocer exactamente cuál es su jornada de trabajo, su horario y el tiempo a disposición de la empresa, así como su descanso diario, semanal o mensual, ya que todo lo que exceda de ello, llamadas al móvil, mensajes de WhatsApp o correos electrónicos, por ejemplo, pueden incluso suponer una vulneración de un derecho fundamental[63].

"A tales efectos, se señala que la tecnología y el acceso a Internet desde cualquier parte del mundo nos han facilitado la vida, el conocimiento y las comunicaciones y nos permite estar permanentemente conectados, pero están afectando a la vida personal y a la conciliación de la vida personal y familiar, con consecuencias cada vez más importantes sobre la salud de los trabajadores. El derecho a desconectar es el derecho del trabajador a conocer su jornada de trabajo, su horario y el tiempo a disposición del empresario, porque fuera del establecimiento del mismo, la intromisión del empresario llamando al trabajador, al móvil, mandándole un WhatsApp o un correo electrónico, es una vulneración del

empresario del tiempo de trabajo. El trabajador también tiene derecho al descanso diario, semanal y mensual, y a conocer la concreción de su jornada de trabajo. El tiempo de trabajo, la jornada laboral, el tiempo de descanso y las

[62]ExtractodeArtículoMonográfico.Noviembre2018Unaaproximaciónalosderechosdigitalesenlanuevaley OrgánicadeProtecciónde DatosJavierPuyolMontero.Abogado.Magistradoexcedente.ConsultorTIC. Director de Puyol-Abogados&Partners

[63] Nota: Cfr. "La desconexión laboral es un derecho fundamental de los trabajadores". Sindicato UGT. Acuerdo 2018-2020. Disponible en: https://goo.gl/xErSEs

jornadas extraordinarias de trabajo (horas extras y horas complementarias) se encuentran regulados en el Estatuto de los Trabajadores, en Reales Decretos específicos (Jornadas especiales, por ejemplo) y en la negociación colectiva. Si termina la jornada laboral, termina. Las nuevas tecnologías deben contribuir a redistribuir los tiempos de trabajo y a crear más empleo".

Por ello, así se reconoce legalmente que los trabajadores y los empleados públicos tienen 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.

En lo que hace referencia a las modalidades de ejercicio de este derecho, las mismas han de atender a la naturaleza y objeto de la relación laboral, potenciando, en todo caso, el derecho a la conciliación de la actividad laboral y la vida personal y familiar.

Del mismo modo, se determina la necesidad de que el establecimiento de estos criterios se sujete a lo establecido en las normas relativas a la negociación colectiva o, en su defecto, a lo acordado, o lo que se pueda acordar al efecto, entre la empresa y los representantes de los trabajadores.

Tampoco puede pasarse por alto la obligación que se atribuye al empleador consistente en que, previa audiencia con los representantes de los trabajadores, proceda a elaborar una política interna dirigida a trabajadores, incluidos los que ocupen puestos directivos, en la que definan las modalidades de ejercicio del derecho a la desconexión, y las acciones de formación y de sensibilización del personal con relación a un uso razonable de las herramientas tecnológicas, que tenga por finalidad evitar el riesgo llamado de "fatiga informática", que consiste en el cansancio que produce manejar excesivas cantidades de datos [Nota: Según una encuesta realizada hace unos años por la agencia de Noticias Reuters, el tener la mente saturada con información hace que muchas personas se sientan estresadas, retrasen decisiones importantes o no presten atención. En otras palabras, la avalancha continua de datos puede desbordarnos y agotarnos mental y físicamente. Los expertos siempre han dicho que tener abundante información ayuda a tomar buenas decisiones.

La Ley Orgánica pone un especial énfasis en el hecho de que se preserve el derecho a la desconexión digital en los supuestos de realización total o parcial del trabajo a distancia, así como en el domicilio del empleado vinculado al uso con fines laborales de herramientas tecnológicas, lo que también supone una importante novedad.

Otra cuestión de suma importancia incluida dentro del marco de los derechos digitales es la que hace referencia al derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo.

De este modo, se reconoce el derecho de los empleadores a 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 art. 20.3 del Estatuto de los Trabajadores y en la legislación de función pública, pero siempre con el condicionamiento que estas funciones se ejerzan dentro de su marco legal y con los límites inherentes al mismo.

DERECHOS QUE ESTÁN INCLUIDOS EN MATERIA PROTECCIÓN DATOS.

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 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. 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 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.

Estás expresamente prohibido en aseos, zonas de descanso y aseos, como especial novedad se permite la grabación de sonido, sin embargo, esta grabación debe estar debidamente justificados.

sometimiento a lo dispuesto en el RGPD, debido a que existe un tratamiento de datos personales. De esta forma, hay que cumplir con la citada norma.

Entre las obligaciones que hay que adoptar estarían, por ejemplo, lo referente tanto al registro de actividades de tratamiento como el derecho el derecho de información, a los que nos hemos referido anteriormente.

- Este punto se podría dividir a su vez en varios más, la AEPD no obstante ha confeccionado una Guía completa[64] para orientar a los interesados de videovigilancia, además ha añadido unas fichas resumidas[65] de fácil lectura y comprensión, además de informes jurídicos y por último resuelven preguntas frecuentes[66] sobre la videovigilancia y su uso correcto.

De lo anterior extraemos la siguiente información:

1.- ¿Es el uso de la videovigilancia, un tratamiento de carácter personal?

La agencia responde: "La imagen es un dato de carácter personal ya que identifica o hace identificable a una persona. En este sentido, la instalación de cámaras, con diversas finalidades como podría ser la seguridad, el control laboral, el acceso a zonas restringidas captando la matrícula del coche y la imagen del conductor, o incluso la monitorización de una UVI, supondría un tratamiento de datos de carácter personal y, en consecuencia, se le aplicaría la normativa de protección de datos."

a) Videovigilancia en el ámbito público

En primer lugar, la videovigilancia sólo debe utilizarse cuando no sea posible acudir a otros medios que causen menos impacto en la privacidad.

Además, no se podrá captar imágenes de la vía pública con fines de seguridad, ya que es competencia de las ([67]Fuerzas y Cuerpos de Seguridad 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), salvo el caso que:

esulte imprescindible para la finalidad que se pretende.
esulte imposible evitarlo por razón de la ubicación de las cámaras.

En todo caso, deberá evitarse cualquier tratamiento de datos innecesario para la finalidad perseguida. Está prohibida la instalación en baños, vestuarios, o lugares análogos.

Por otra parte, el tratamiento de las imágenes con fines de seguridad mediante la videovigilancia debe adecuarse al RGPD, de manera que, en primer lugar, hay que configurar el registro de actividades de tratamiento regulado en el artículo 30 del RGPD.

Asimismo, se tiene que dar cumplimiento al derecho de información del artículo 13. Para ello se puede optar por un sistema de capas de la siguiente forma:

---

[64] https://www.aepd.es/media/guias/guia-videovigilancia.pdf
[65] https://www.aepd.es/areas/videovigilancia/index.html
[66] https://sedeagpd.gob.es/sede-electronica-web/vistas/infoSede/preguntasFrecuentes.jsf
[67] https://boe.es/buscar/doc.php?id=BOE-A-1997-17574, ley de videovigilancia FCS. 24/10/2019

- Colocar un cartel donde aparezca que es una zona videovigilada, la identidad del responsable y la posibilidad del ejercicio de los derechos previstos en los artículos 15 a 22 del RGPD.
- Mantener a disposición de los afectados el resto de información referida en el artículo 13.

También se deberán adoptar las medidas de seguridad, teniendo en cuenta lo siguiente: El artículo 32 del RGPD determina que se establezcan las medidas técnicas y organizativas apropiadas para garantizar el nivel de seguridad adecuado al riesgo.

Por otra parte, lo previsto en el Esquema Nacional de Seguridad es aplicable a cualquier información de las Administraciones Públicas sin distinción del soporte en el que se encuentre, por lo que en cuanto a las medidas de seguridad se refiere, este esquema es acorde al enfoque de riesgo del RGPD y se constituye en una herramienta válida para la gestión del riesgo y la adopción de las medidas de seguridad en las citadas Administraciones. Por tanto, la implementación de las medidas de seguridad cuando se lleve a cabo un tratamiento de datos mediante el uso de la videovigilancia dependerá del análisis de riesgo llevado a cabo previamente.

No obstante, cuándo se trate de tratamientos de videovigilancia que entrañen un escaso riesgo, como podría ser el caso de uso en comunidades de propietarios o pequeños establecimientos, puede utilizarse la herramienta de esta AEPD denominada FACILITA_RGPD.

Por otra parte, si se encarga a un tercero la gestión de las cámaras, estaremos ante la figura del encargado del tratamiento, quién deberá cumplir los requisitos que regula el artículo 28 del RGPD.

sometimiento a lo dispuesto en el RGPD, debido a que existe un tratamiento de datos personales. De esta forma, hay que cumplir con la citada norma.

Entre las obligaciones que hay que adoptar estarían, por ejemplo, lo referente tanto al registro de actividades de tratamiento como el derecho el derecho de información, a los que nos hemos referido anteriormente.

b) Videovigilancia en el ámbito doméstico: [68]

- Cámara instalada en el interior de mi vivienda, cuando la captación de imágenes se limite exclusivamente al interior de la vivienda se considera que se realiza en el ejercicio de una actividad personal o doméstica, a la que no le es aplicable esta normativa.
- Sólo se aplicará el RGPD y la LOPDGDD, cuando las cámaras puedan captar imágenes de personas en el exterior de la vivienda (entradas, fachadas, medianerías,).

[68] https://www.aepd.es/media/fichas/ficha-videovigilancia-mi-vivienda.pdf

- Las imágenes captadas por las cámaras se limitarán a la vivienda de la que se sea titular. No podrán captarse imágenes de la vía pública a excepción de una franja mínima de los accesos a la vivienda. Tampoco podrán captarse imágenes de terrenos y viviendas colindantes o de cualquier otro espacio ajeno.
- Si se utilizan cámaras orientables y/o con zoom será necesaria la instalación de máscaras de privacidad[69] para evitar captar imágenes de la vía pública, terrenos y viviendas de terceros.
- Las imágenes serán conservadas durante un plazo máximo de un mes desde su captación, transcurrido el cual se procederá al borrado.

✓ ¿Se aplica la normativa de protección de datos a la instalación de las videocámaras ficticias?

Al tratarse de cámaras simuladas, no captarían imágenes de personas físicas identificadas o identificables, por lo que, al no quedar acreditada la existencia de un tratamiento de datos personales, la cuestión se encuentra al margen de la normativa de protección de datos.

✓ Tengo instalada una cámara con fines de seguridad que no graba, sólo permite el visionado en tiempo real. ¿Tengo que cumplir alguna obligación?

En aquellos supuestos en que las cámaras no graban imágenes, pero sí se permite la reproducción en tiempo real de las mismas, también supone un sometimiento a lo dispuesto en el RGPD, debido a que existe un tratamiento de datos personales. De esta forma, hay que cumplir con la citada norma.

Entre las obligaciones que hay que adoptar estarían, por ejemplo, lo referente tanto al registro de actividades de tratamiento como el derecho el derecho de información, a los que nos hemos referido anteriormente.

✓ Quiero poner una cámara en una moto para grabar mis viajes. ¿Es legal esta captación?

La normativa de protección de datos no es de aplicación a los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas.

En el caso planteado, se podría aplicar la excepción doméstica y realizar la grabación de los viajes, siempre y cuando dicha grabación fuese para uso estrictamente personal.

No obstante, si, por ejemplo, las grabaciones se publicasen en Internet, supondría un desvío de la finalidad doméstica, por lo que sí sería de aplicación la normativa de protección de datos personales.

[69] http://ingenieria.tvc.mx/kb/a2079/configuracion-mascara-de-privacidad-en-camaras-ip.aspx, ¿cómo configurar la máscara de privacidad en mi cámara.

c) Videovigilancia en el ámbito laboral

¿puede mi empresa establecer un sistema de videovigilancia en mi lugar de trabajo? ¿Es necesario mi consentimiento? ¿Qué uso pueden dar a las imágenes?

El Estatuto de los Trabajadores faculta al empresario para adoptar las medidas que estime más oportunas para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, que deberán guardar la consideración debida a la dignidad humana y tener en cuenta la capacidad real de los trabajadores con discapacidad.

- Los sistemas de videovigilancia para control empresarial sólo se adoptarán cuando exista una relación de proporcionalidad entre la finalidad perseguida y el modo en que se traten las imágenes y no haya otra medida más idónea.

- Se tendrá en cuenta el derecho a la intimidad y a la propia imagen de los trabajadores. Se prohíbe su instalación en baños o vestuarios.

- En todos los casos se deberá informar de la existencia de un sistema de videovigilancia. A este fin se colocará un cartel suficientemente visible en los accesos a las zonas vigiladas, que indicará de forma clara la identidad del responsable de la instalación, ante quién y dónde dirigirse para ejercer los derechos que prevé la normativa de protección de datos, y dónde obtener más información sobre el tratamiento de los datos personales. La AEPD pone a su disposición un modelo de cartel. Igualmente, se pondrá a disposición de los afectados el resto de la información a la que se refiere el artículo 13 del Reglamento General de Protección de Datos. (Sin embargo, parecer que esta apreciación que se realiza por parte de la AEPD, no es absoluta y a la vista de la sentencia del Tribunal Europeo de Derechos Humanos – en el asunto de las cajeras de Mercadona conocida como “López Ribalda”, si existen sospechas razonables de la comisión de ilícitos y la medida es proporcional se permite el uso de cámaras ocultas)[70]
- También habrá de informarse personalmente a los trabajadores y a la representación sindical, por cualquier medio que garantice la recepción de la información. Nunca deberá efectuarse a direcciones particulares de los trabajadores ni a través de llamadas a sus móviles privados.

[70] http://noticias.juridicas.com/actualidad/noticias/14509-el-tedh-cambia-de-criterio:-grabar-a-empleados-con-camara-oculta-no-vulnera-su-intimidad-en-ciertas-circunstancias/
Enlace de la sentencia https://www.icav.es/bd/archivos/archivo11428.pdf

- Así mismo, se pondrá a disposición de los afectados la restante información que exige artículo 13 del Reglamento General de Protección de Datos

¿Se aplica la normativa de protección de datos a la instalación de las videocámaras ficticias?

Al tratarse de cámaras simuladas, no captarían imágenes de personas físicas identificadas o identificables, por lo que, al no quedar acreditada la existencia de un tratamiento de datos personales, la cuestión se encuentra al margen de la normativa de protección de datos.

 Tengo instalada una cámara con fines de seguridad que no graba, sólo permite el visionado en tiempo real. ¿Tengo que cumplir alguna obligación?

En aquellos supuestos en que las cámaras no graban imágenes, pero sí se permite la reproducción en tiempo real de las mismas, también supone un sometimiento a lo dispuesto en el RGPD, debido a que existe un tratamiento de datos personales. De esta forma, hay que cumplir con la citada norma.

Entre las obligaciones que hay que adoptar estarían, por ejemplo, lo referente tanto al registro de actividades de tratamiento como el derecho el derecho de información, a los que nos hemos referido anteriormente.

 Quiero poner una cámara en una moto para grabar mis viajes. ¿Es legal esta captación?

La normativa de protección de datos no es de aplicación a los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas.

En el caso planteado, se podría aplicar la excepción doméstica y realizar la grabación de los viajes, siempre y cuando dicha grabación fuese para uso estrictamente personal.

No obstante, si, por ejemplo, las grabaciones se publicasen en Internet, supondría un desvío de la finalidad doméstica, por lo que sí sería de aplicación la normativa de protección de datos personales

- **¿Qué pasa si se capta un hecho ilícito con estas cámaras?**

Se permite el uso de estas imágenes siempre que se informe a los empleados, sin necesidad de consentimiento y por otro lado se entiende información suficiente el establecimiento de cartel informativo en un lugar visible.

Evolución jurisprudencial

- ✓ La sentencia STC 2/09/2013 "Universidad de Sevilla"
- ✓ STC 03/03/2016 "Caso Bershka"
- ✓ STEDH 9/01/18 "López Ribalda"
- SJS nº3 de Pamplona, sobre el despido de un trabajador por una pelea 19/02/2019[71]

Se debe informar previamente de en dicha sentencia FJ2,F) establece la aplicación de las exigencias derivadas de la jurisprudencia y la normativa, "*Los anteriores razonamientos determinan que en el presente caso deba ratificarse la decisión adoptada en el propio acto del juicio de inadmitir la prueba consistente en el visionado de las grabaciones realizadas por las cámaras de seguridad de la empresa demandada, y ello porque la empresa demandada no cumplió las exigencias vinculadas al necesario respeto al derecho de protección de datos que amparaba al trabajador demandante, incluyendo el deber informativo sobre la existencia de sistema de videovigilancia y la propia finalidad para la que se utilizaba , incluyendo la posibilidad de sancionar si captan actos ilícitos o incumplimientos laborales . Hay que destacar que los hechos que han dado lugar al despido disciplinario del trabajador son anteriores a la entrada en vigor de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Y, desde esta perspectiva temporal, ni siquiera la nueva regulación es aplicable al caso enjuiciado a pesar de la alegación realizada en el acto del juicio por la empresa demandada. Y tampoco se estima aplicable la doctrina que cita de la STC 39/2016 porque en los términos razonados lo cierto es que el deber informativo sobre el alcance de las medidas de videovigilancia, incluyendo la finalidad sancionadora, es una exigencia que se impone en todo caso , más allá de la mera colocación del cartel informativo, conforme a la jurisprudencia del Tribunal Europeo de Derechos Humanos y el propio Reglamento General de Protección de Datos a que se ha hecho referencia, que obligan a su aplicación y a interpretar la propia normativa nacional en los términos que exige el TEDH y que se derivan del Reglamento Europeo, dotado de eficacia directa y primacía frente a la norma nacional que contradiga su contenido, teniendo en cuenta que en dicho reglamento"*

[71] http://www.supercontable.com/boletin/A/sentencias_boletin/SJS_PAMPLONA_11_2019.pdf

JURISPRUDENCIA

No se establece excepción alguna al deber de transparencia e informativo en materia de protección de datos aplicable a las relaciones laborales, sin embargo tras la sentencia del Tribunal de derechos Humanos respecto al caso “López Ribalda” se autoriza el uso de cámaras ocultas cuando existan indicios claros de ilícito penal “ sí existe esta sospecha razonable (no sirve al efecto una mínima sospecha o suposiciones), la instalación de cámaras ocultas para vigilar a los empleados es lícita y por ello, las pruebas obtenidas a través de dichas grabaciones son válidas ante los Tribunales” además de lo anterior se exige que se supere el juicio de proporcionalidad (medida proporcional, idónea y necesaria).

DERECHO A LA UTILIZACIÓN DE SISTEMAS DE GEOLOCALIZACIÓN EN EL TRABAJO.ART89

Necesidad de información previa del uso que se va a dar a este sistema de geolocalización, es decir si se aplicaría alguna medida disciplinaria en el uso de este dispositivo.

Se reforman estatutos de los trabajadores y estatuto del empleado público. "Sobre la base de este derecho, debe tenerse presente que se reconoce el derecho de los empleadores a 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 art. 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.

A los efectos procedimentales de la puesta en marcha de este derecho se exige que, con carácter previo, los empleadores tienen que proceder a informar de forma expresa, clara e inequívoca a los trabajadores o los empleados

públicos y, en su caso, a sus representantes, con relación a la existencia y características de estos dispositivos.

Igualmente, se determina que esta información que se proporcione debe versar sobre el posible ejercicio de los derechos de acceso, rectificación, limitación del tratamiento y supresión"[72].

Resolución Agencia Española Protección de datos, uso geolocalización Policía Ayto. AP/61/18, vulneración del art.4 anterior ley protección datos.

Sentencia de AN 6 febrero 2019, "¿es legal que Telepizza obligue a sus repartidores a aportar su teléfono móvil y a usar sus datos tarifarios de internet para geolocalizar los pedidos que entregan en beneficio de la empresa?" El debate jurídico gira alrededor del proyecto Tracker Reparto de Telepizza, instaurado con la finalidad de que los clientes que usasen este servicio pudiesen geolocalizar los pedidos a domicilio en tiempo real. Cuya conclusión es:

"El proyecto instaurado por la empresa consistente en geolocalizar a los repartidores cuando realicen tareas de reparto mediante una app descargada en su teléfono móvil personal, no respeta el derecho a la privacidad de los trabajadores por cuanto que no supera el juicio de proporcionalidad[73]"

[72]file:///C:/Users/velor/AppData/Local/Packages/Microsoft.MicrosoftEdge_8wekyb3d8bbwe/TempState/Downloads/DOCUMENTO%20SEPIN%20SP-DOCT-81150%20(1)%20(1).pdf ArtículoMonográfico.Noviembre2018SP/DOCT/81150UnaaproximaciónalosderechosdigitalesenlanuevaLeyOrgánicadeProtecciónde DatosJavierPuyolMontero.Abogado.Magistradoexcedente.ConsultorTIC.Directorde Puyol-Abogados&Partners

[73] https://www.laboral-social.com/sites/laboral-social.com/files/NSJ059450.pdf Sentencia de la AN utilización del sistema geolocalización por Telepizza. Sentencia 13/2019 del 6 de Febrero 2019.

Este derecho trajo consigo modificaciones en materia laboral, en los estatutos del trabajador tanto privado (TREETT nuevo art.20) como público (TREBEP nueva j) bis art.14), ambos modificados por las DF13 y DF14 respectivamente.

Muy ligado al control por geolocalización de los trabajadores viene dado el control laboral mediante datos biométricos, preguntas muy habituales respecto el uso de esos métodos y la legitimación de la empresa para ejercerlo, la necesidad o no de consentimiento previo o si estos datos son necesarios para ejercer ese control laboral espero puedan ser resueltos a continuación: ¿pueden utilizar datos biométricos como la huella digital en el control horario? ¿es necesario que de mi consentimiento? ¿se entendería legítimo dicho consentimiento?
Real Decreto-ley 8/2019, de 8 de marzo, de medidas urgentes de protección social y de lucha contra la precariedad laboral en la jornada que entró en vigor a partir del 12 de mayo de 2019, obliga a los empresarios a registrar el horario de cada empleado, es una obligación que establece al empleador por tanto abre la polémica de cuál es el medio más adecuado para realizar ese control.

La AEPD determina que la empresa podrá habilita el sistema que considere más adecuado y por tanto, desde la perspectiva fundamental de la protección de datos, tendrían la misma base de legitimación y no precisarían el tratamiento consensuado con los trabajadores los sistemas manuales, analógicos o digitales al efecto de generar la prueba justificativa del registro diario de la jornada de cada trabajador, que deberá estar a disposición tanto de los propios trabajadores como de la inspección de trabajo y los representantes legales de los trabajadores y deberá almacenarse un periodo de 4 años.[74]

Con carácter general y para la implementación del registro de jornada no se precisa el consentimiento del trabajador, siendo base suficiente de legitimación la propia norma laboral, que en el artículo 34.9 ET establece la obligación de las empresas de realizar dicho registro de la jornada con carácter individual de cada persona trabajadora y que, de acuerdo con lo previsto en el artículo 6.1.c del Reglamento europeo 2016/679 (RGPD), el tratamiento de datos personales de los trabajadores derivado de la implantación del registro de jornada es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento. No obstante, lo anterior, la existencia de una lícita condición para el tratamiento de los datos de los empleados sin necesidad del consentimiento de los trabajadores no excluye el deber de las empresas de informar a los trabajadores de la existencia del registro y de la finalidad del tratamiento de los datos personales individuales que se obtienen con dicho registro.

[74] https://sedeagpd.gob.es/sede-electronica-web/vistas/infoSede/detallePreguntaFAQ.jsf;jsessionid=1SwwdaHpyVEcc17D2c5ha2uZ?idPregunta=FAQ%2F00275

¿Pero esta legitimación da vía libre para que se pueda utilizar datos biométricos para ese control horario? ¿Qué consecuencias tiene el uso de estos datos?[75]

Tal y como adelanta el Sr García herrero, "ese interés legítimo, en el ámbito de RRHH, vendrá normalmente acompañado de la excepción recogida en el artículo 9.2.b) del Reglamento General de Protección de Datos".

Pero, leyendo bien "porque la excepción b) bien leída, e interpretada en relación con el considerando 41, el artículo 88, ambos del Reglamento General de Protección de Datos y el artículo 53 de la Constitución Española, arrojan la conclusión de que la norma habilitante de este tratamiento RRHH tiene que tener rango de ley".

"Y en la medida en que ni la nueva LOPDGDD, ni -para el caso- ninguna otra norma con rango de ley autoriza expresamente el tratamiento de datos biométricos en el ámbito laboral, la otra posibilidad de norma habilitante con rango de ley."

Es por esto que se entiende que deberían ser objeto de negociación colectiva y aprobarlo por convenio laboral y así se habilitaría ese tratamiento con una norma con rango de ley.

La agencia de protección de datos se ha pronunciado la agencia catalana concreta que:

"Una vez que los datos biométricos han pasado a ser considerados como datos especialmente protegidos, no parece tan claro que la utilización de sistemas de control horario basados en este tipo de datos deben ser admitidos como medio preferente para llevar a cabo dicho control. ***Más bien al contrario***. Dada la especial naturaleza de estos datos parece que habrá que optar en primer lugar por otros sistemas de control que, sin utilizar categorías de datos en mente protegidos, puedan permitir alcanzar el mismo fin.*"*

- ¿pero qué pasa si pedimos el consentimiento de los trabajadores para legitimar el tratamiento de datos art. 6RGPD?

Bien, definiremos el consentimiento como art.4.11 y art.7 RGPD como "toda manifestación de voluntad, específica, informada e inequívoca, por la que el interesado acepta el tratamiento".

- ¿Pero el consentimiento en el sector público es un consentimiento válido?

Según el profesor Lorenzo Cotino Hueso y en interpretación de la STC 292/2000, "el tratamiento de datos de carácter personal siempre, que no haya consentimiento, es un acto de constricción, de restricción de este derecho de carácter personal, necesita de una ley que establezca esas garantías de esa restricción"

[75] https://jorgegarciaherrero.com/politica-de-desconexion-digital-novedades-en-geolocalizacion-y-control-de-jornada-laboral/

C 42: El consentimiento no debe considerarse libremente prestado cuando el interesado no goza de verdadera o libre elección o no puede denegar o retirar su consentimiento sin sufrir perjuicio alguno.

C43: Para garantizar que el consentimiento se haya dado libremente, este no debe constituir un fundamento jurídico válido para el tratamiento de datos de carácter personal en un caso concreto en el que exista un desequilibro claro entre el interesado y el RT, en particular cuando dicho responsable sea una autoridad pública y sea por lo tanto improbable que el consentimiento se haya dado libremente en todas las circunstancias de dicha situación particular. Se presume que el consentimiento no se ha dado libremente cuando:

- no permita autorizar por separándolas distintas operaciones de tratamiento de datos personales pese a ser adecuado en el caso concreto,
- o cuando el cumplimiento de un contrato, incluida la prestación de un servicio, sea dependiente del consentimiento, aun cuando este no sea necesario para dicho cumplimiento

Entendiendo por tanto que, si hay un desequilibrio claro, hay una relación asimétrica y por tanto ese consentimiento estaría viciado y no sería válido. Por ejemplo: En una relación laboral hay un desequilibrio claro de punto de partida.

Por tanto, el tratamiento de la huella como dato biométrico deberá fundarse en una obligación legal art. 8 LOPDGDD y 6 RGPD, que como hemos visto si estaría justificado el control horario, pero no el uso de huellas para ese tratamiento, salvo que fuera el único modo de cumplir o que las otras alternativas, tarjetas magnéticas o perforadas, no son por alguna razón de peso, suficientes para cumplir dicho interés.

Entonces sería la empresa la que debería justificar según lo establecido en el art. 9.2 LOPDGDD la base jurídica legal que justifican el tratamiento de datos mediante ese sistema tan invasivo. Que no cabría otra que la aprobación por convenio, mediante negociación colectiva, del uso de estos datos como medio de control horario

Derecho de olvido en búsquedas a internet art.93 y Derecho olvido en redes sociales art.94

Art. 93:

1. Toda persona tiene 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. Del mismo modo deberá procederse cuando las circunstancias personales que en su caso invocase el afectado evidenciasen la prevalencia de sus derechos sobre el mantenimiento de los enlaces por el servicio de búsqueda en Internet. Este derecho subsistirá aun cuando fuera lícita la conservación de la información publicada en el sitio web al que se dirigiera el enlace y no se procediese por la misma a su borrado previo o simultáneo.

2. El ejercicio del derecho al que se refiere este artículo no impedirá el acceso a la información publicada en el sitio web a través de la utilización de otros criterios de búsqueda distintos del nombre de quien ejerciera el derecho.

Art.94:

1. Toda persona tiene 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.

2. Toda persona tiene derecho a que sean suprimidos los datos personales que le conciernan y que hubiesen sido facilitados por terceros para su publicación por los servicios de redes sociales y servicios de la sociedad de la información equivalentes 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. Del mismo modo deberá procederse a la supresión de dichos datos cuando las circunstancias personales que en su caso invocase el afectado evidenciasen la prevalencia de sus derechos sobre el mantenimiento de los datos por el servicio. Se exceptúan de lo dispuesto en este apartado los datos que hubiesen sido facilitados por personas físicas en el ejercicio de actividades personales o domésticas.

3. En caso de que el derecho se ejercitase por un afectado respecto de datos que hubiesen sido facilitados al servicio, por él o por terceros, durante su minoría de edad, el prestador deberá proceder sin dilación a su supresión por su simple solicitud, sin necesidad de que concurran las circunstancias mencionadas en el apartado 2[76].

[76] cve: BOE-A-2018-16673 Verificable en http://www.boe.es

- ¿Cómo ejercer este derecho? Nivel práctico[77].

Derecho al olvido ante los buscadores

Existe muchos buscadores, pero los más populares ya ofrecen un formulario traducido para que sus usuarios europeos puedan ejercer el derecho al olvido fácilmente.

Para ello, accederemos al formulario perteneciente a cada buscador donde queremos ejercer nuestro derecho, por ejemplo:

GOOGLE: Acceso para solicitar la eliminación de contenido indexado en sus búsquedas.

YAHOO: Solicitudes para Bloquear resultados de búsqueda en Yahoo! Search.

BING: Solicitud para bloquear resultados de búsqueda en Bing en Europa.

A continuación, rellenaremos los datos que nos solicitan, como nuestro nombre completo. Además, en caso de solicitarlo para otra persona, nos identificaremos como solicitud en “Actúo en nombre de…”.

también debemos indicar cuál es la URL que queremos eliminar y por qué. En este apartado tenemos que ser muy concretos con el motivo por el que se solicita la eliminación del enlace.

En el siguiente apartado demostraremos nuestra identidad y para ello tendremos que adjuntar una imagen de nuestro Documento Nacional de Identidad.

Marcaremos la casilla de conformidad donde consentimos que se procese la información y, por último, firmaremos nuestra solicitud.

En el caso de que los buscadores no ofrezcan respuesta a dicha petición, podremos pedir a la Agencia Española de Protección de Datos que tutele nuestro derecho frente al buscador a través de este formulario.[78]

BOLETÍN OFICIAL DEL ESTADO Núm. 294 Jueves 6 de diciembre de 2018 Sec. I. Pág. 119840

[77] https://www.osi.es/es/actualidad/blog/2018/09/19/sabes-como-ejercer-el-derecho-al-olvido extracto de artículo Instituto Nacional de Ciber seguridad.

[78] https://www.aepd.es/reglamento/derechos/index.html#anchor3 Formularios para ejercer tu derecho de supresión.

Testamento digital

Artículo 96. Derecho al testamento digital[79].

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 hubiera 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.

[79] BOLETÍN OFICIAL DEL ESTADO Núm. 294 Jueves 6 de diciembre de 2018 Sec. I. Pág. 119841

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.

IX. REFLEXIONES.

Está claro que esta materia no es especialmente novedosa, pero al parecer respecto al tratamiento de protección de datos y el respeto a estos, estamos todavía muy poco maduros a nivel social.

Hay que destacar, que hablar de protección de datos es hablar de una dualidad, la que representa el RGPD y la LOPDGDD ya que estas normativas van unidas y buscan continuamente complementarse, el amplio catalogo de considerando del RGPD es una fuente importante de interpretación y se hace indispensable para poder comprender el interés y objetivo del legislador a nivel europeo y al mismo tiempo el del legislador a nivel Estatal.

Tras la aprobación del Reglamento, existe la obligación legal de complementación y desarrollo normativo y sobre todo respecto a la inclusión de cuadro infractor, esta inclusión de infracciones y de sanciones en la actual normativa, ha supuesto una llamada de atención y parece haber despertado en la mayoría de empresas un incipiente interés en actualización normativa y adaptación al RGPD, no es para menos, recordemos las cuantías de estas sanciones podrían suponer hasta 20 millones de euros. Pero desgraciadamente y desde mi punto de vista, todavía queda muchísimo para que se cumpla a raja tabla lo que se expone en la ley. Quizás el que no se dote de recursos humanos a la AEPD, puede provocar que se pierda este "especial" respeto a la norma, pues se aprecie falta de efectividad por parte del organismo de control que avoque a un incumplimiento sistemático.

Sería interesante la posibilidad de un canal directo entre la agencia y los ciudadanos no solo de denuncias sino informativo, la AEPD ya dispone de un apartado de FAQS pero que recoge aquellas consultas realizadas por los responsables y encargados de datos, así como de los DPD.

Tampoco contribuye a un efectivo cumplimiento, los continuos vaivenes jurídicos, y es que desde la implementación de la actual ley de protección de datos ya ha habido más de una resolución en uno u otro sentido, como ya hemos visto el uso de la videovigilancia o la cesión de datos a partidos políticos.

Por otra parte, parece ser que todo es dato y tratamiento, pero no debemos perder de vista que es solo una parte de un gran todo, como se aprecia en resoluciones como la del "**uso de una cámara de videovigilancia ficticia**"[80], la imagen como dato es solo una perspectiva de protección, no debemos olvidar conceptos como la protección a la intimidad y la limitación en el uso de la informática, que aunque no están dentro del ámbito jurídico de protección LOPDGDD y el RGPD y por tanto de la AEPD, son esferas que en ocasiones se solapan.

[80] http://noticias.juridicas.com/actualidad/noticias/14602-una-camara-falsa-disuasoria-apuntada-a-una-finca-privada-tambien-supone-una-intromision-a-la-intimidad/

El hecho de que algo no esté incluido en las leyes de protección en materia de datos no significa que esté exento de protección, por lo que deberemos buscar otras vías de defensa como la jurisdiccional en los casos de vulneración de derechos laborales con el uso de la video vigilancia.

Queda claro por tanto que no todo es dato personal y que la disección del concepto de dato personal debe ser clara en cuanto a la adopción de medidas que garanticen su defensa, no obstante, en ocasiones se hace complicada pues la imagen, la intimidad y el honor pueden confluir con el derecho de control sobre nuestros datos y hacer difícil su disección. Por tanto, la visión más correcta es la cual la protección de datos es una parcela que forma parte de un todo, en la que se aplica, como ya hemos apuntado antes, una defensa administrativa frente la jurisdiccional de otros, sin olvidar que la protección de datos consiste en un poder de disposición y de control sobre los datos, que faculta a la persona a decidir cuáles son los datos que se va a tratar o recabar por un tercero y su uso.

La protección de datos como trabajo ha supuesto un desafío, no tanto respecto a la falta de información (estamos ante una normativa reciente aprobada) sino a la excesiva información; el mundo de las tecnologías suponen un gran avance y posibilita el acceso a millones de datos e información, pero también un desafío respecto a la selección y la asunción de los mismos, no obstante el que la normativa no tenga ni un año de vigencia contribuye también a que la mayoría de dicha información supusiera artículos de opinión, noticias de actualidad y sentencias, las cuales aclaraban o resolvían aquellos flecos que la propia norma no dejaba claro.

La posibilidad de adquirir unas habilidades en materia de protección y seguridad informática, unida a un conocimiento de nuestro derechos y garantía digitales supondrá el ejercicio de un poder directo sobre nuestros datos. Es por esto que en materia de la protección de datos hay que ir más allá del desarrollo normativo, la nueva LOPDGDD ya establece unas bases de desarrollo que supondrán la incorporación de la educación digital como asignatura y como requisito para el acceso incluso a la función pública; parece mentira que estemos plenamente inmersos en ella, pero todavía no sepamos controlarla.

La tecnología es impresionante, supone un avance para humanidad en su conjunto, para mí siempre a sido una materia de especial interés todo lo tecnológico me atrae de igual manera que ocasiones me produce un gran vértigo y rechazo, el desarrollo de los nuevos modos de comunicación con la aparición primera de los móviles y ahora los smartphones me generan una gran curiosidad, sin embargo nunca antes me había planteado tan en serio, lo que supone esa inclusión en todo lo “Smart”, todo lo inteligente, y el peaje que pagamos respecto a nuestra privacidad y la cesión de datos.

Otras de las reflexiones que me surgen es en cuanto a edad mínima, que la propia norma establece para que el consentimiento sea válido, se establece en nuestra normativa a 14 años, en mi opinión una edad demasiado temprana o al menos no considero que tengan la madurez suficiente para poder decidir sobre el uso de sus datos y ni siquiera que sean capaces de comprender la complejidad del tratamiento, el RGPD acota la edad y la sube a mayores de 16 años en mi opinión quizá una edad más adecuada.

El uso de los dispositivos móviles en menores es cada vez más extendido, desde mi punto de vista es una contradicción que se proporcione teléfonos móviles con acceso a internet a menores de 12, 10, 13 años o incluso 14, el porqué de esta formulación tiene varias respuestas conectada una a la otra: la primera que simplemente carecen de la información esencial para proteger su intimidad, sus datos y protegerse de ciertos peligros que supone el mundo del internet. La normativa consciente de esto, establece unas bases que sirvan para desarrollar esa labor educativa en los centros escolares, centros universitarios e incluso incorporarlos a materias de especial transcendencia para el desarrollo de funciones en la Administración Pública.

Por otra parte, en mi trabajo, observo como la brecha generacional entre padres e hijos se hace patente en diferentes ámbitos, pero donde más se pronuncia es en el uso de las tecnologías, los padres, caben excepciones, se presentan sobrepasados y abatidos por la realidad, sus hijos son víctimas de delitos y agresiones y no son capaces de explicar o advertir sobre el uso de las tecnologías, no saben como funcionan las mayorías de aplicaciones y no tienen claras las garantías y medios de protección frente a esas amenazas. La AEPD está haciendo una labor espectacular respecto esto, en ocasiones sobrepasando sus competencias, pero es importante que todos tanto los adultos como los jóvenes conozcan de los peligros y sepan utilizar las herramientas que disponen para evitar estas situaciones.

Por otra parte, resulta característico que en pleno desarrollo tecnológico no se haya conseguido avanzar y conectar a aquellas partes del territorio, hablo del español en este caso, que se encuentran totalmente aislados y no solo por su situación geográfica respecto del resto, sino porque no disponen de lo más elemental en este momento digital que es cobertura.

En la ley se hace alusión a esto, casi como una necesidad, creo que es importante que esa conexión se desarrolle por igual, la garantía de los derechos digitales debe proveer a todos los ciudadanos de unos mínimos y entre ellos debe estar la posibilidad del uso del internet como herramienta básica.

Por último, me gustaría que se desarrollase mejor la figura del Delegado de Protección de datos, que se resolvieran dudas respecto a su configuración dentro del mundo profesional de los datos, que se aclarasen dudas sobre la capacitación mínima necesaria, los conocimientos mínimos de derecho, el grupo o estatus laboral al que debe pertenecer, si bien la AEPD ha dado detalles como en es el caso de la Administración pública que debe pertenecer a un grupo A1 no se aclara bien el tipo de régimen jurídico laboral que deben adoptar para su

inclusión en estas, para dotarlo de esa independencia debería ser funcionario público o adoptar como hacen muchas administraciones la opción de contratación externalizada.

Indudablemente este trabajo me ha dotado de ciertos conocimientos para una mejor defensa, pero si me preguntaran que uniría a esta ley de protección de datos y al RGPD sería sin duda un MASTER en seguridad informática o digital

X. BIBLIOGRAFÍA.

1. Reig, J. B., & Leal, Á. J. (2010). *La protección jurídica de la intimidad*. Iustel.
2. VID. En este sentido la Entrevista a Mar España directora de la AEPD, extracto de la Obra "Especial nueva Ley Orgánica de protección de datos y garantía de los derechos digitales", Wolters Kluwer 11 de diciembre de 2018.
3. Delgado, Lucrecio Rebollo, y María Mercedes Serrano Pérez. "*Introducción a la protección de datos"*. Editorial Dykinson, s.l.i, 2010, pag.25
4. Delgado, Lucrecio Rebollo. *Vida privada y protección de datos en la Unión Europea*. Dykinson, Madrid, 2008, pág. 102
5. Muñoz, Alfonso Galán. *La protección jurídica de la intimidad y de los datos de carácter personal frente a las nuevas tecnologías de la información y comunicación*. Tirant lo Blanch, 2014.
6. Extracto de la Obra "Primer Congreso Nacional de DPOs. Wolters Kluwer". Pag 32 Davara Rodriguez, Miguel Ángel (2018) DPO: "Cuestiones de interés en materia de formación y certificación". Madrid.
7. «Las relaciones entre el Derecho Comunitario y el Derecho interno de los Estados miembros a la luz de la Jurisprudencia del Tribunal de Justicia», Mangas Martín, dentro de la obra colectiva El Derecho Comunitario Europeo y su aplicación judicial, editado por el CGPJ, la Universidad de Granada y la editorial Civitas, Madrid, 1993, pág. 81
8. ExtractodeArtículoMonográfico.Noviembre2018. "Una aproximaciónalosderechosdigitalesenlanuevaLeyOrgánicadeProtecciónd eDatos" JavierPuyolMontero. Abogado. Magistrado excedente. Consultor TIC. Director de Puyol-Abogados&Partners
9. Guía práctica de Protección de datos en el ámbito Sanitario. Editorial Sepin.S. L 2019. Las Rozas (Madrid)

Revisados 01/12/2019.

1. Fuente CIS, Barómetro de mayo de 2018 http://datos.cis.es/pdf/Es3213mar_A.pdf
2. https://www.aepd.es/media/guias/guia-ciudadano.pdf Guía práctica de la AEPD
3. Extracto entrevista a la presidenta AEPD Mar España, incluida en la obra "Especial Ley Orgánica de Protección de datos y derechos digitales" Wolters Kluwer diciembre 2018 https://www.smarteca.es/my-

reader/SMT2018025_00000000_0?fileName=content%2FEX0000140123_20181210.HTML&location=pi-493&publicationDetailsItem=SystematicI

4. Programa FACILITA, consulta15/04/2019 https://www.servicios.agpd.es/AGPD/view/form/MDAwMDAwMDAwMDAwMDIxNzcxMjkxNTU1Mjg2NTYzMDI3?updated=true

5. Estudio sobre protección de datos de la AEPD, abril y mayo de 2018, consulta el 15/04/2019 https://www.aepd.es/media/estudios/estudio-proteccion-de-datos-aepd-cepyme.pdf

6. El creador de la 'World Wide Web' crea una nueva red que da a los usuarios control sobre sus datos https://www.lavanguardia.com/tecnologia/20181001/452114001384/creador-internet-crea-red-usuarios-control-datos. Ese artículo se desprende de este otro artículo original https://www.fastcompany.com/90243936/exclusive-tim-berners-lee-tells-us-his-radical-new-plan-to-upend-the-world-wide-web (fecha consulta 12 marzo 2019

7. Sentencia 94/98 del 24 de Mayo Tribunal Constitucional sobre el control sobre los datos http://hj.tribunalconstitucional.es/HJ/eu-ES/Resolucion/Show/SENTENCIA/1998/94

8. https://forma2.inap.es/c4x/AEPD/AEPD19-01/asset/Webminar_1.pdf, curso sobre protección de datos de la AEPD para empleados de la administración local, del epígrafe **"Desligando algunos derechos**", exposición. Eduard Chaveli Donet, 2019.

9. https://www.boe.es/buscar/doc.php?id=BOE-A-1982-11196, **ley para la protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen.**

10. Vid. En el mismo sentido este artículo cuando se trata de estudios o estadísticas y siempre que los datos estén anonimizados de manera tal que sea imposible su reconocimiento a posteriori https://www.lavanguardia.com/vida/20191029/471274125624/ine-seguira-movimientos-moviles-estudio.html el INE seguirá movimientos móviles, para estudiar mejor en infraestructuras, 2019 Noviembre

11. (https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_es)

12. (https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_es)

13. El 01/10/2019 en sentencia el TJUE (ECLI:EU:C: 2019:801) ASUNTO C-673/17, decisión planteada por el Bundesgerichsthof (Alemania)el Tribunal Supremo de lo Civil y Penal, Alemania sobre el uso de COOKIES. En dicha sentencia declara que el consentimiento que el usuario de un

sitio de internet debe dar para la colocación de cookies en su equipo o terminal y la consulta de éstas no es válida con la mera marcación por defecto de una casilla y retirarla si no desea su consentimiento. El tribunal subraya que el consentimiento debe ser específico, de modo que el hecho de que un usuario active el botón de en la participación en el juego organizado con fines promocionales no basta para considerar que éste se ha dado de manera su consentimiento para la colocación de cookies. Además, según el Tribunal de justicia, la información que le proveedor de servicios debe facilitar al usuario incluye tiempo durante el cual las cookies estarán activas y la posibilidad de que terceros tengan acceso a ellas. Extracto de noticias jurídicas http://noticias.juridics.com/actualidad/jurisprudencia/1445-la-colocacion-de-cookies-requiere-el-consentimiento-activo-de-los-internautas.

14. https://www.samuelparra.com/wp-content/uploads/2010/08/archivo_denuncia-matricula.pdf Procedimiento E/01173/2009 del 1 de Julio de 2009 en el que se aclara que "la comunicación mediante la colocación de la denuncia en el parabrisas del vehículo de la denunciante (refiriéndose a la persona que interpuso la denuncia en la AEPD), se ha de señalar que el citado boletín no refleja dato personal alguno de la denunciante, en la medida en la que los datos incluidos en el no permite su identificación "Por otro lado respecto a la licitud del tratamiento sin consentimiento, el informe señala " (…) en principio, sólo se puede llevar a cabo (…) con el consentimiento del titular" sin embargo señala que existen determinados casos en el que los datos de un particular no requieran de la autorización previa exigida como regla general" poniendo como ejemplo " dichos datos de carácter personal se recojan para el ejercicio de las funciones propias de la Administración públicas, cuestión tal que se observa en el presente caso" fecha consulta 15/04/2019.

15. https://www.boe.es/boe/dias/2019/06/25/pdfs/BOE-A-2019-9548.pdf LEY ORGÁNICA DE PROTECCIÓN DE DATOS Y GARANTIAS DE DERECHOS DIGITALES.

16. http://curia.europa.eu/juris/liste.jsf?language=es&num=C-131/12, Sentencia SSTJ GoogleSpain y Google Inc. contra AEPD, ámbito Territorial y Material 13 mayo 2014. Sentencia de Google Spain.

17. Consultada la página de la AEPD, fecha de consulta 15/04/2019 https://www.aepd.es/agencia/transparencia/organigrama/direccion.html

18. https://www.boe.es/boe/dias/2018/12/06/pdfs/BOE-A-2018-16673.pdf LOPDGDD.Regulados en los artículos 71,72,73 y 74 LOPDGDD y en el RGPD 83.5, 83.4,83.6, las sanciones prescriben: a) Las sanciones por importe igual o inferior a 40.000 euros, prescriben en el plazo de un año. b) Las sanciones por importe comprendido entre 40.001 y 300.000 euros prescriben a los dos años. c) Las sanciones por un importe superior a 300.000 euros prescriben a los tres años. 2. El plazo de prescripción de

las sanciones comenzará a contarse desde el día siguiente a aquel en que sea ejecutable la resolución por la que se impone la sanción o haya transcurrido el plazo para recurrirla.

19. https://www.boe.es/buscar/doc.php?id=BOE-A-2018-16673 Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, consulta 13/04/19.

20. http://www.lssi.gob.es/paginas/Index.aspx Ley de servicios de la sociedad de la información y del comercio electrónico.

21. https://www.aepd.es/media/guias/guia-rapida-dpd.pdf guía sobre cómo se debe realizar la comunicación del DPO, realizada por la AEPD consulta 15/04/2019.

22. Vid. Este artículo hace especial incidencia en el ámbito de aplicación de la normativa en materia de protección de datos realizando una clara diferenciación en cada uno de los ámbitos, https://www.iberley.es/temas/objeto-ambito-aplicacion-rgpd-lopdgdd-62715 desarrollo del ámbito subjetivo y objetivo de la LOPDGDD Y RGPD, extraído de la obra lBERLEY "Objeto y ámbito de aplicación del Reglamento General de protección de Datos (RGPD) y de la LO 3/2018 de 5 de diciembre de protección de datos (LOPDGDD), COLEX, fecha consulta 13/04/2019.

23. Ley Orgánica 6/1985, de 1 de julio. LO del Poder Judicial.

24. ¿Qué es un Considerando? Cada una de las razones que apoyan o sirven de fundamento al texto de una ley o a una sentencia, auto, decreto o resolución. Recibe dicho nombre por ser ésta la palabra con que comienza, http://www.enciclopedia-juridica.com/d/considerando/considerando.htm

25. (Sentencia Avon, respecto la resolución de AEPD imposición de dos sanciones de 28.000 euros, falta de consentimiento e inexactitud, Audiencia Nacional, Sentencia 25 septiembre 2019) https://diariolaley.laleynext.es/content/Documento.aspx?params=H4sIAAAAAAAAAEAMtMSbH1CjUwMDAzMTc2NzFWK0stKs7Mz7Mty0xPzStJBfEz0ypd8pNDKgtSbdMSc4pT1TKLHQsKivLLUlNsjQwMLQ0NDC0MDQ0MAKwec6lMAAAAWKE

26. https://diariolaley.laleynext.es/content/Documento.aspx?params=H4sIAAAAAAAAAEAMtMSbH1CjUwMDAzMTc2NzFWK0stKs7Mz7Mty0xPzStJBfEz0ypd8pNDKgtSbdMSc4pT1TKLHQsKivLLUlNsjQwMLQ0NDC0MDQ0MAKwec6lMAAAAWKE Registro de actividades de tratamiento inventario de la AEPD

27. http://www.europarl.europa.eu/factsheets/es/sheet/157/la-proteccion-de-los-datos-personales,consulta 18/03/2019

28. https://eur-lex.europa.eu/legal-content/es/ALL/?uri=CELEX%3A12012E%2FTXT18/03/2019

29. http://www.europarl.europa.eu/charter/pdf/text_es.pdf18/03/2019

30. https://www.boe.es/eli/es/lo/2018/12/05/3 consulta el 13/04/2019

31. https://www.aepd.es/media/guias/guia-modelo-clausula-informativa.pdf consulta 13/04/2019.

32. Antonio Pérez Van Kappel, que cita la Sentencia de 5-4-79 (Ratti) -, «El efecto directo del Derecho de la Unión Europea», Cuadernos Digitales de Formación, Espacio judicial europeo social. III Edición (2013-2014), Consejo General del Poder Judicial.

33. Preámbulo de la ley 3/2018 de 3 de diciembre, LOPDGDD https://www.boe.es/eli/es/lo/2018/12/05/3/con consultada el 13/04/2019.

34. https://www.boe.es/boe/dias/1998/06/09/pdfs/T00008-00013.pdf sentencia TC 94/1998.

35. https://www.boe.es/eli/es/lo/2018/12/05/3/con LOPDGDD estructura principal de la norma y resumen de los propósitos de desarrollo de cada uno de los títulos, fecha de consulta 13/04/2019

36. http://www.privacidadlogica.es/crossover-entre-el-rgpd-y-la-nueva-lopd/ Crossover LOPD Y RGPD, por Publicado el 13 de diciembre de 2018 por Francisco Javier Sempere.

37. https://protecciondatoslopd.com/empresas/conservarciondatosplazo/#Ley_Organica_de_Proteccion_de_Datos,consulta 14/04/2019.

38. https://www.aepd.es/reglamento/derechos/index.html, consulta 14/04/2019.

39. https://www.google.com/webmasters/tools/legalremovalrequest?complaint_type=rtbf&visit_id=636908020850650508-67773449&rd=1, fecha de consulta 14/04/2019.

40. https://www.youtube.com/reportingtool/legal, consulta 14/04/2019.

41. “marco legislativo local y nacional” Curso protección de datos INAP, a funcionarios de las AAPP Locales, epígrafe Derechos Digitales. 25/10/2019.

42. https://www.boe.es/eli/es/rdlg/2000/08/04/5/con Real Decreto Legislativo 5/2000, de 4 de agosto, por el que se aprueba el texto refundido de la Ley sobre Infracciones y Sanciones en el Orden Social.

43. https://ecodiario.eleconomista.es/espana/noticias/7638101/06/16/Clan-y-la-AEPD-lanzan-una-campana-de-educacion-digital-para-fomentar-el-buen-uso-de-Internet-y-las-redes-sociales.html

44. https://www.aepd.es/prensa/2019-07-29-aepd-anar-mar-espana-carta-derechos-ninos-adolescentes.html

45. https://elderecho.com/control-por-parte-de-la-empresa-del-correo-electronico-del-empleado

46. http://www.poderjudicial.es/search/contenidos.action?action=contentpdf&databasematch=AN&reference=8741724&statsQueryId=120795116&calledfrom=searchresults&optimize=20190425 Sentencia 28/03/2019 Andalucía STSJ

47. "La desconexión laboral es un derecho fundamental de los trabajadores". Sindicato UGT. Acuerdo 2018-2020. Disponible en: https://goo.gl/xErSEs

48. http://www.supercontable.com/boletin/A/sentencias_boletin/SJS_PAMPLONA_11_2019.pdf

49. file:///C:/Users/velor/AppData/Local/Packages/Microsoft.MicrosoftEdge_8wekyb3d8bbwe/TempState/Downloads/DOCUMENTO%20SEPIN%20SP-DOCT-81150%20(1)%20(1).pdf ArtículoMonográfico.Noviembre2018SP/DOCT/81150Unaaproximaciónalosderechosdigitalesenlanuevaley Orgánicade Protección de Datos. JavierPuyolMontero. Abogado. Magistradoexcedente.ConsultorTIC.Directorde Puyol-Abogados&Partner

50. https://www.laboral-social.com/sites/laboral-social.com/files/NSJ059450.pdf Sentencia de la AN utilización del sistema geolocalización por Telepizza. Sentencia 13/2019 del 6 de febrero 2019.

51. cve: BOE-A-2018-16673 Verificable en http://www.boe.es

52. BOLETÍN OFICIAL DEL ESTADO Núm. 294 jueves 6 de diciembre de 2018 Sec. I. Pág. 119840

53. https://www.osi.es/es/actualidad/blog/2018/09/19/sabes-como-ejercer-el-derecho-al-olvido extracto de artículo Instituto Nacional de Ciber seguridad.

54. https://www.aepd.es/reglamento/derechos/index.html#anchor3 Formularios para ejercer tu derecho de supresión

55. BOLETÍN OFICIAL DEL ESTADO Núm. 294 jueves 6 de diciembre de 2018 Sec. I. Pág. 119841

XI. ANEXOS. Implementación RGPD Y LOPDGDD a una pequeña empresa

Como punto final incluyo en el apartado de anexos el presente trabajo, un ejemplo de lo que podría ser la implementación a una pequeña empresa el RGPD y la LOPDGDD.

En este caso el responsable es el señor Juan Tudesca Almansa, quién realiza el tratamiento de datos en el ejercicio comercial de su empresa, para poder realizar su actividad principal que es la venta de electrodomésticos, el señor Juan Tudesca tiene que recopilar datos Nombre y apellidos, NIF, domicilio completo y correo electrónico para enviarles las facturas al mismo.

En principio su legitimación vendría dada por el cumplimiento del servicio u contrato de compraventa y respaldado por el interés legítimo del responsable de datos, según establece el considerando 47 del RGPD, este interés legítimo vendría dado por el contrato de compra-venta realizado por el responsable y el cliente.

Las cláusulas legales pertinentes.

INFORMACIÓN BÁSICA DE PROTECCIÓN DE DATOS

RESPONSABLE: TU ELECTRODOMESTICO S.L

FINALIDAD: prestar servicio, podría incluir alguna comunicación posterior para realizar un seguimiento y encuesta de satisfacción por la compra.

LEGITIMACIÓN: ejecución del contrato de servicio, además del interés legítimo del responsable según se desprende del considerando 47 RGPD

DESTINATARIOS: los datos proporcionados solo serán cedidos al fabricante para activar la garantía de la misma. Por lo que puede suponer la cesión a terceros países ya que algunos de los productos suministrados por el responsable son fabricados en países no pertenecientes a la Unión Europea, no obstante, dicha cesión solo se realizará para cumplir con la garantía del producto suministrado. Los terceros países son los siguientes:

Le informamos que los datos serán transferidos a una entidad ubicada en ARGENTINA, país que garantiza un nivel de protección adecuado, según decisión de la Comisión.

Le informamos que los datos serán transferidos a una entidad en ECUADOR con la que se ha establecido un contrato que incluye las cláusulas tipo de protección de datos adoptadas por la Comisión y que puede consultarse en www.OLX.com/tid

DERECHOS: se podrán ejercer derechos de acceso, rectificación y supresión de datos, tal y como se explica en la información adicional, (ARCO).

INFORMACIÓN ADICIONAL: puede consultar la información detallada de protección de datos en WWW.TU ELECTRODOMESTICO S.L /protecciónde datos

En esta página y en el epígrafe de tratamiento de datos se relacionarán los derechos con más profundidad:

- Derecho a solicitar el acceso a los datos personales relativos al interesado,
- Derecho a solicitar su rectificación o supresión,
- Derecho a solicitar la limitación de su tratamiento,
- Derecho a oponerse al tratamiento
- Derecho a la portabilidad de los datos

DPO: Se podrá ejercer los derechos a través de la cuenta de correo

protecciónde datos@dpotuelectrodoméstico.es o si esa gestión ha sido encomendada a mi persona como gestora de datos vlrodpo@hotmail.es

PLAZO DE CONSERVACIÓN DE LOS DATOS: Este plazo varía dependiendo de la obligación que se pretenda cumplir por parte del empresario, aunque a efectos fiscales solo haría necesario la conservación de las facturas y libros 5 años, el código de comercio, sin embargo, establece en Artículo 30. 1. Los empresarios conservarán los libros, correspondencia, documentación y justificantes concernientes a su negocio, debidamente ordenados, durante seis años, a partir del último asiento realizado en los libros, salvo lo que se establezca por disposiciones generales o especiales.

Por otra parte, en cuanto el cumplimiento en base a la ley de impuesto de sociedades, deberá atenerse a un plazo más amplio si están aplicando compensación de bases imponibles negativas, siendo este de 10 años.

Por otra parte, está el cumplimiento de la Ley General de Defensa de Consumidores y Usuarios establece una garantía de dos años para los electrodomésticos nuevos, sin embargo, la garantía ampliada de los productos suministrados por nuestro cliente tiene una duración de 10 años (no obstante, esta garantía debe solicitarse directamente al fabricante)

TRATAMIENTO AUTOMATIZADO: Se informa al interesado de que sus datos

NO serán tratados de manera automatizada.

- ***El Registro de Actividades de Tratamiento.***

.

RESPONSABLE DEL TRATAMIENTO

- Datos identificativos del responsable del tratamiento: TU ELECTRODOMESTICO S.L., con NIF B34222980 y domicilio en C/ Mayor, 28 · 34001 Palencia.
- Datos identificativos del Delegado de Protección de Datos (si corresponde): Verónica López Rodríguez, 48659205X, Avd. GRAN CAPITÁN 10,1 IZQ (MADRID), vlrodpo@hotmail.es

DESCRIPCIÓN DE LA ACTIVIDAD DE TRATAMIENTO

Actividad de tratamiento	• Gestión de clientes • Gestión de proveedores
Finalidad	• Realización de servicio de compra-venta • Servicio de garantía
Interesados	• Clientes • Proveedores
Categorías de datos	• Datos identificativos • Datos contables (facturación) • Datos referencia productos, imei, etc.

TRANSFERENCIAS INTERNACIONALES Y CESIONES

Cesiones	• Identificación de proveedores • Olux (Ecuador) • ATMA (Argentina) • LG (Yeongdeungpo-gu, Corea del Sur)y a su sede en MADRID
Transferencias previstas	Detalle de las transferencias internacionales de datos previstas: países, legitimación, etc En nuestro caso sería el cumplimiento de las garantías del fabricante, según el considerando 47 RGPD.
Periodo de conservación	Plazo previsto para la conservación de la información: • En cumplimiento de la obligación fiscal y de

	5 facturación años • En cumplimiento de la obligación de cobertura de garantía 2 años • En cumplimiento de la ley de comercio 6 años • En cumplimiento ley impuesto de sociedades 10 años.

CICLO DE VIDA DE LA ACTIVIDAD DE TRATAMIENTO

CAPTURA DE LOS DATOS

Actividades del proceso	Detalle de los procesos que intervienen en la captura de la información: formularios, contratos, facturas, encuestas de satisfacción que se proporcionarán preferentemente a través de la página web.
Datos tratados	Tipos de datos que se recopilan: Nombre y apellidos, NIF, domicilio completo y correo electrónico • Datos de necesarios para reparación, número referencia productos.
Intervinientes	Personas y usuarios que intervienen en la recogida de la información • Señor Juan Tudesca Almansa • ASESORIA ALEGRE S.L., con NIF B34590782 y domicilio en C/ Manoteras, 27 · 34008 Palencia) por la facturación. • RESPALDO REMOTO S.L. NIF B47679430 y domicilio en Av. América, 34 · 47020 VALLADOLID). • proporcionado por la empresa SERVICIOS INTERNET S.L., con NIF B28396980 y domicilio en Av. Libertad, 38 · 28057 Madrid. • DESARROLLOS CAMPO S.L. con NIF B34678930 y domicilio en Av. Valladolid, 34 · 34002 Palencia. • Transportista: Juan Luis Terranilla Pérez, con NIF 12879720V y domicilio en C/ La fuente, 34 · 34011 Palencia).

Tecnologías	Tecnología que interviene en la recogida de la información • Backup • Ordenador de sobremesa con Windows 10 • correo electrónico • programa informático FACTURAWIN • ADSL y wifi

ALMACENAMIENTO DE LOS DATOS	
Actividades del proceso	Detalle del proceso de almacenamiento de la información: • se realiza copia de seguridad en Backup externa mediante la empresa contratada para ello. • Se almacena también datos de manera externa a través de la asesoría, para servicio de facturación.
Datos tratados	Tipos de datos que se almacenan Nombre y apellidos, NIF, domicilio completo y correo electrónico • Datos de necesarios para reparación, número referencia productos.
Intervinientes	Personas y usuarios que intervienen en el almacenamiento de la información • RESPALDO REMOTO S.L. NIF B47679430 y domicilio en Av. América, 34 · 47020 VALLADOLID). • (ASESORIA ALEGRE S.L., con NIF B34590782 y domicilio en C/ Manoteras, 27 · 34008 Palencia).
Tecnologías	Tecnología que interviene en el

	almacenamiento de la información • Backup • ordenador de sobremesa con Windows 10 • correo electrónico • ADSL y wifi

USO Y TRATAMIENTO DE LOS DATOS

Actividades del proceso	Detalle de los diferentes usos de la información: • Gestionar el registro del Usuario • Gestionar las incidencias y reparaciones de los productos • Atender las consultas, sugerencias y quejas que el Usuario ponga en conocimiento • Facturación • Envío de productos a domicilio a través servicio de transporte
Datos tratados	Tipos de dato Nombre y apellidos, NIF, domicilio completo y correo electrónico • Datos de necesarios para reparación, número referencia productos que se gestionan:
Intervinientes	Personas y usuarios que intervienen en la gestión de la información: • Señor Juan Tudesca Almansa • ASESORIA ALEGRE S.L., con NIF B34590782 y domicilio en C/ Manoteras, 27 · 34008 Palencia) por la facturación. • RESPALDO REMOTO S.L. NIF B47679430 y domicilio en Av. América, 34 · 47020 VALLADOLID).

	• proporcionado por la empresa SERVICIOS INTERNET S.L., con NIF B28396980 y domicilio en Av. Libertad, 38 · 28057 Madrid. • DESARROLLOS CAMPO S.L. con NIF B34678930 y domicilio en Av. Valladolid, 34 · 34002 Palencia. • Transportista: Juan Luis Terranilla Pérez, con NIF 12879720V y domicilio en C/ La fuente, 34 · 3
Tecnologías	Tecnología que interviene en el uso de la información: • Backup • ordenador de sobremesa con Windows 10 • correo electrónico • ADSL y wifi

5. DESTRUCCIÓN

Actividades del proceso según UNE-EN 15713:2010.	Detalle del proceso de destrucción de la información: • Se destruirá mediante el borrado de archivos digitales, se encomienda esa destrucción a la empresa RESPALDO REMOTO S.L. • Los datos que se encuentren en formato papel a través de una destructora de papel que el responsable tiene en la empresa.
Datos tratados	Tipos de datos que se destruyen: • Datos identificativos • Datos contables (facturación) • Datos referencia productos, imei, etc.

	Los soportes serán: Papel En medios electrónicos y digitales
Intervinientes	Personas y usuarios que intervienen: • RESPALDO REMOTO S.L. • Juan Tudesca Almansa
Tecnologías	Tecnología que interviene en la destrucción de la información: Destructora Rexel RLX20 Hojas: 22 Corte: Partículas Corte: 4x40 mm. Capacidad Papelera: 115 litros Nivel DIN: P-4

MEDIDAS DE SEGURIDAD DEL RESPONSABLE DE TRATAMIENTO

Se tratará los datos del Usuario en todo momento de forma confidencial y guardando el preceptivo deber de secreto respecto de los mismos, de conformidad con lo previsto en la normativa de aplicación, adoptando al efecto las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de sus datos y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos.