GRADO EN DERECHO

TRABAJO DE FIN DE GRADO

NUEVA REGULACIÓN SOBRE PROTECCIÓN DE DATOS Y DERECHO AL OLVIDO

(Data Protection Regulation and Right to be Forgotten)

Autora: Rocío Castaño Romero

Tutor: Pedro Martínez Ruano. Área de Derecho Constitucional.

Convocatoria: Junio 2018

RESUMEN

Este trabajo aborda la nueva normativa europea sobre protección de datos. Intentando dar alcance a los objetivos, así como a las numerosas novedades que aporta el Reglamento. Analizando los nuevos derechos regulados, y los mecanismos que deben desarrollar las empresas para cumplir con el Reglamento General de Protección de Datos. Además se estudia el Proyecto de Ley Orgánica de Protección de Datos que se está debatiendo en el Congreso, y las diferencias con la anterior legislación. Por último, se investiga acerca del derecho al olvido, su origen y evolución.

This thesis is about General Data Protection Regulation. Trying to achieve the goals and the variety of the news introduced by the new Regulation. It analyzes new rights and how business should obey with GDPR. Moreover, it is focused on the Spanish Law on Data Protection. Lastly, it knows about the right to be forgotten

INTRODUCCIÓN.

Desde hace unas décadas a la actualidad las nuevas tecnologías han supuesto un enorme cambio en la sociedad. Han afectado desde las relaciones personales, al desarrollo de las funciones laborales, así como han abierto nuevos campos de actuación que hasta hace unos años eran impensables como comprar por Internet o pagar a través de nuestro teléfono móvil.

Por lo tanto, con la realización de determinados actos o actividades a través de las nuevas tecnologías, enviamos innumerables datos de carácter personal o bien a empresas, o simplemente se quedan divagando por el abstracto mundo de Internet.

Según la Agencia Española de Protección de Datos, los datos de carácter personal son "*cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables*."

La protección de datos ya en nuestra Constitución de 1978, fue considerada como un Derecho Fundamental. Casi 50 años después y con el enorme avance tecnológico que se ha desarrollado en estos años, la protección de los datos personales debe tener un alcance mucho mayor, porque están mucho más expuestos.

El Derecho no es "*norma y solo norma"* como afirmara en su Teoría Pura del Derecho Hans Kelsen, sino que las normas surgen como respuesta a cambios sociales, económicos, políticos, culturales o morales. El Derecho debe ir al mismo paso que la sociedad, no debe quedarse por detrás.

En este contexto la Unión Europea crea el Reglamento 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)

Introduciendo numerosas novedades, y figuras desconocidas hasta el momento siendo la misión de este Trabajo, acercarnos al nuevo régimen jurídico de protección de datos.

CAPITULO I. EL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS.

1. Introducción.

A mediados de 1800 en Estados Unidos, el Juez Thomas Cooley dijo una frase que pasaría a la Historia, "*el derecho a no ser molestado*". En un principio se interpretó como el posible nacimiento del derecho a la protección de datos, pero realmente estaba en el contexto de "el derecho de la persona se dice que es el derecho a la completa inmunidad; a ser dejado solo" por lo que Thomas Cooley se refería al derecho individual a la inmunidad personal frente a agresiones físicas. [1] Pero de alguna forma Thomas Cooley impulsó a los que se consideran los padres del derecho a la protección de datos y a la intimidad: Samuel Warren y Louis Branderis.

Ambos se sentían amenazados por esa evolución tecnológica de finales del siglo XIX. La llegada del telégrafo o de la fotografía suponía un riesgo para la difusión de información de carácter personal. Esta preocupación la dejaron plasmada en su famoso ensayo de la siguiente forma:

"Los recientes inventos y los nuevos métodos de hacer negocios fueron los focos de atención en el siguiente paso que hubo de darse para amparar a la persona, y garantizar al individuo lo que el juez Cooley denomina el derecho «a no ser molestado». Las instantáneas fotográficas y las empresas periodísticas han invadido los sagrados recintos de la vida privada y hogareña; y los numerosos ingenios mecánicos amenazan con hacer realidad la profecía que reza: «lo que se susurre en la intimidad, será proclamado a los cuatro vientos» […] La intensidad y la complejidad de la vida, que acompañan a los avances de la civilización, han hecho necesario un cierto distanciamiento del mundo, y el hombre, bajo la refinada influencia de la cultura, se ha hecho más vulnerable a la publicidad, de modo que la soledad y la intimidad se han convertido en algo esencial para la persona; por ello, los nuevos modos e inventos, al invadir su intimidad, le producen un sufrimiento espiritual y una angustia mucho mayor que la que le pueden causar los meros daños personales".[2]

---

[1] SALDAÑA M.N. «The Right to Privacy» La génesis de la protección de la pricacidad en el sistema constitucional norteamericano.: El centenario legado de Warren y Brandeis. UNED. Revista de Derecho Político, nº85. Septiembre-Diciembre 2012, p. 206.

[2] WARREN, S. D. y BRANDEIS, L. D. (1995). *El derecho a la intimidad.*, págs. 26 y 27. Para la edición original, «The Right to Privacy», pág. 196.

La respuesta para esta inmediata invasión debía ser la creación de un principio que protegiera a los ciudadanos de éstas nuevas tecnologías que estaban cayendo en la mano del hombre. De tal forma que así fue como nació lo que hoy día conocemos como "derecho a la protección de datos".

Así fue como intimidad y protección de datos nacieron unidos. Pero es necesario concebirlos de forma complementaria y no unitaria (como pasó durante un tiempo en España). El derecho a la intimidad concibe su máxima en la expresión "mi casa es mi castillo"[3], es decir, nadie tiene porque saber o conocer lo que ocurre en el interior de mi hogar, o de mi mismo. Concibiendo hogar no solo como algo material o relacionado con la propiedad, sino también de modo espiritual. Y el derecho a la protección de datos es ese rastro de información que vamos dejando por el camino con la realización de actividades de la vida cotidiana.

2. La protección de datos en la Constitución Española de 1978.

La Constitución Española regula en su artículo 18.4 el derecho fundamental a la protección de datos con la siguiente redacción: *"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".*

Fue llamativo, desde un primer momento, que nuestra Constitución diera tal relevancia al concepto dado el año en el que fue elaborada (1978) y como los constituyentes supieron apreciar el riesgo que iba a suponer el uso de la informática.

Se trataba de un derecho incipiente, totalmente novedoso y que en gran medida carecía de un contenido material. El origen europeo del derecho a la protección de datos tiene acento alemán. En primer lugar, porque fue en Alemania donde se llevo a cabo la primera ley sobre protección de datos en 1970, conocida como "Datenschutzgesetz" y que supuso un hito, pues hasta el momento no había habido ninguna norma dedicada en exclusiva a la protección de datos.

En segundo lugar es importante destacar la jurisprudencia del Tribunal Constitucional Federal de Alemania con la sentencia del 15 de Diciembre de 1983 de la denominada "Ley del Censo", donde se reconoció que cada individuo tiene derecho a saber lo que se

[3] Para un estudio de los orígenes de la máxima inglesa «*home is your castle*»,. FLAHERTY, D.H. (1972). *Privacy in Colonial New England.*, págs. 85-88.

sabe de él. Concretamente estipulaba que *"la autodeterminación del individuo presupone – también las condiciones de las técnicas modernas de tratamiento de la información que se concede al individuo la libertad de decisión sobre las acciones que vaya a realizar, o en su caso, a omitir, incluyendo la posibilidad de obrar de hecho en forma consecuente con la decisión adoptada. Esta libertad de decisión, de control, supone además que el individuo tenga la posibilidad de acceder a sus datos personales, que pueda, no solo tener conocimiento de que otros procesen informaciones relativas a sus persona, sino también someter del uso de éstas a un control, ya que de lo contrario se limitara su libertad de decidir por autodeterminación."* [4]

Por lo tanto, la Constitución española (1978) junto con la portuguesa (1976) sembraron los precedentes constitucionales para lo que con posterioridad se conocería como el derecho a la protección de datos.

Con la regulación de este derecho el constituyente intentaba dar respuesta a un problema cada vez más común en nuestra sociedad: los ciudadanos no controlamos la mayor parte de la información que existe sobre nosotros. Materialmente, los ciudadanos hemos perdido el control de nuestra intimidad, lo que es un riesgo de la sociedad de la información. [5]

Pero el entorno normativo del derecho a la protección de datos, en un principio, fue un poco caótico. Dado que se tendía a solapar derecho a la intimidad (18.1 CE) y derecho a la protección de datos (18.4 CE), pues en un principio se entendía el derecho a la protección de datos como una especificación del derecho a la intimidad. [6]

De tal forma que desde 1978, cuando entró en vigor la Constitución hasta principios de los años 90 no se entendió como un derecho autónomo e independiente. Hasta el punto que su primera ley orgánica de desarrollo no fue hasta 1992 con la LORTAD.

Poco tiempo después de la entrada en vigor de la LORTAD, el Tribunal Constitucional dictó la sentencia 254/1993 que empezaría a aclarar las dudas acerca de este derecho,

---

[4] Traducido por DARANAS, M.(enero 1984). BJC. Nº33. Véase HEREDERO HIGUERAS, M.; *"La sentencia del TC de la República Federal Alemana relativa al censo de población de 1983*". Documentación administrativa. Nº 198, páginas 139-158.

[5] PEREZ ROYO, J.; "Curso de Derecho Constitucional", Ed: Marcial Pons, Madrid, 2016, p.311.

[6] Véase, http://www.congreso.es/consti/constitucion/indice/sinopsis/sinopsis.jsp?art=18&tipo=2

principalmente identificando el contenido del artículo 18.4 CE como un derecho fundamental.

"*Dispone el art. 18.4 C.E. 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". De este modo, nuestra Constitución ha incorporado una nueva garantía constitucional, como forma de respuesta a una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona, de forma en último término no muy diferente a como fueron originándose e incorporándose históricamente los distintos derechos fundamentales. En el presente caso estamos ante un instituto de garantía de otros derechos, fundamentalmente el honor y la intimidad, pero también de un instituto que es, en sí mismo, un derecho o libertad fundamental, el derecho a la libertad frente a la potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos, lo que la Constitución llama "la informática".*[7]

"Es suficiente con constatar que, al negarse a comunicarle la existencia e identificación de los ficheros automatizados que mantiene con datos de carácter personal, así como los datos que le conciernen a él personalmente, la administración demandada en este proceso vulneró el contenido esencial del derecho a la intimidad del actor, al despojarlo de su necesaria protección"[8]

Lo que nos viene a decir esta sentencia es que el derecho del artículo 18.4 es una garantía para proteger el derecho al honor y a la intimidad fundamentalmente. De tal forma que por un lado lo ensalza como un derecho fundamental pero por otro lado lo une indudablemente a la intimidad; porque la interpretación que hace el Tribunal Constitucional es que se produce una vulneración del derecho a la intimidad cuando se le niega la comunicación e identificación de los ficheros que contienen sus datos personales. Por lo tanto, ésta sentencia dibuja un panorama de luces y sombras entorno al derecho a la protección de datos, también denominado derecho a la autodeterminación informativa o derecho a la libertad informática.

Pero es indispensable citar ésta sentencia (STC 254/1993) pues fue la primera en la materia en España, reconociendo la protección de datos como derecho fundamental,

[7] Véase, Sentencia Tribunal Constitucional 254/1993, de 20 Julio. FJ 6.
[8] Véase, Sentencia Tribunal Constitucional 254/1993, de 20 Julio. FJ 8.

aunque en ese momento fuera denominado "libertad informática" y no fuese definido de forma clara por ésta jurisprudencia.

Pero si hay una sentencia importante y definitiva respecto a la protección de datos esa es, sin lugar a dudas, la STC 292/2000 de 30 de Noviembre. Y lo es por varias razones:

- En primer lugar porque establece sin género de dudas que la protección de datos es un derecho fundamental en sí mismo, repitiendo, las palabras ya expuestas por la STC 254/1993 FJ 6 (arriba concretado).
- En segundo lugar porque fija el objeto de este derecho fundamental. "*Garantizar a una persona un poder de control sobre sus datos de carácter personal, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derechos del afectado. De este modo, el objeto de protección del derecho fundamental a la protección de datos no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual, que para ello está la protección que el art. 18.1 C.E. otorga, sino los datos de carácter personal. Por consiguiente, también alcanza a aquellos datos personales públicos, que por el hecho de serlo, de ser accesibles al conocimiento de cualquiera, no escapan al poder de disposición del afectado porque así lo garantiza su derecho a la protección de datos. También por ello, el que los datos sean de carácter personal no significa que sólo tengan protección los relativos a la vida privada o íntima de la persona, sino que los datos amparados son todos aquellos que identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo*"[9]
- En tercer lugar porque clarifica el limite o las diferencias existentes entre el derecho a la intimidad y el derecho a la protección de datos. Así que la sentencia señaló que mientras la función de la intimidad era la de proteger al individuo frente a intromisiones no deseadas que pudieran realizarse en su vida personal y familiar, lo que otorgaba a ese derecho un contenido negativo, la protección de

[9] Véase, Sentencia Tribunal Constitucional 292/2000, de 30 de Noviembre. FJ 6.

datos le daba un poder de control sobre sus datos de carácter personal, tanto privados como públicos. [10]

Literalmente estipula la sentencia: "*Este derecho fundamental a la protección de datos, a diferencia del derecho a la intimidad del artículo 18.1 CE, con quien comparte el objetivo de ofrecer una eficaz protección constitucional de la vida privada personal y familiar, atribuye a su titular un haz de facultades que consiste en su mayor parte en el poder jurídico de imponer a terceros la realización u omisión de determinados comportamientos, cuya concreta regulación debe establecer la ley, aquella que conforme al artículo 18.4 CE debe limitar el uso de la informática, bien desarrollando el derecho fundamental a la protección de datos (art. 81.1 CE), bien regulando su ejercicio (art. 53.1 CE). La peculiaridad de este derecho fundamental a la protección de datos respecto de aquel derecho fundamental tan afín como es el de la intimidad radica, pues, en su distinta función, lo que apareja, por consiguiente que también su objeto y contenido difieran"*[11]

Este límite o diferencia ha sido ampliado con el tiempo por la propia doctrina estableciendo que el objeto de la protección de datos es más amplio que el de la intimidad pues alcanza tanto a los datos íntimos como a los datos públicos, porque el carácter íntimo de un dato no es el factor determinante para acordar la protección. Lo definitivo es que se trate de un dato personal, revelador de información sobre una persona y que esa información pueda afectar al ejercicio de nuestros derechos. [12]

- En cuarto lugar especifica el contenido del derecho, haciendo referencia a los conocidos como "derechos ARCO" (acceso, rectificación, cancelación y oposición). "*El contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales para decidir cuáles de esos datos proporcionar a un tercero, o cuales puede este*

[10] MARTINEZ, R. El derecho fundamental a la protección de datos: perspectivas. *IDP. Revista de Internet, Derecho y Politica (5):* p. 47-61. 2007. (Fecha de consulta: 1 de Mayo de 2018). Disponible en: http://www.redalyc.org/articulo.oa?id=78812861005

[11] Véase, Sentencia Tribunal Constitucional 292/2000 de 30 de Noviembre. FJ 5.

[12] GARCIA GUERRERO, J.L. *Los derechos fundamentales a la vida, la igualdad y los derechos de libertad.* Ed. Tirant lo Blanch, Valencia, 2013, p-487.

tercero recabar, y que permite saber quien posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso"[13]

- En quinto lugar, no se trata de un derecho fundamental absoluto. No existen derechos fundamentales absolutos, porque siempre van a estar limitados por otros derechos. *"…este Tribunal ha declarado que el derecho a la protección de datos no es ilimitado, y aunque la Constitución no le imponga expresamente límites específicos, ni remita a los Poderes Públicos para su determinación como ha hecho con otros derechos fundamentales, no cabe duda de que han de encontrarlos en los restantes derechos fundamentales y bienes jurídicos constitucionalmente protegidos, pues así lo exige el principio de unidad de la Constitución (STC 11/1981, de 8 de abril, FJ 7; 196/1987, de 11 de diciembre, FJ 6); y respecto del art. 18, la STC 110/1984, FJ 5). Esos límites o bien pueden ser restricciones directas del derecho fundamental mismo, a las que antes se ha aludido o bien pueden ser restricciones al modo, tiempo o lugar de ejercicio del derecho fundamental. En el primer caso, regular esos límites es una forma de desarrollo del derecho fundamental. En el segundo, los límites que se fijan lo son a la forma concreta en la que cabe ejercer el haz de facultades que compone el contenido del derecho fundamental en cuestión, constituyendo una manera de regular su ejercicio, lo que puede hacer el legislador ordinario a tenor de lo dispuesto en el art. 53.1 CE. La primera constatación que debe hacerse, que no por evidente es menos capital, es que la Constitución ha querido que la Ley, y sólo la Ley, pueda fijar los límites a un derecho fundamental…"*

En definitiva la sentencia 292/2000 deja clara la naturaleza de la protección de datos como derecho fundamental independiente y diferente a la intimidad y también de la privacidad, reconociéndole un ámbito de actuación más extenso que estos dos últimos.[14]

Porque en palabras del Magistrado PABLO LUCAS MURILLO DE LA CUEVA: "En ese empeño, no hay que olvidar que el derecho a la autodeterminación informativa es un derecho fundamental. Que se dirige a satisfacer una necesidad básica de toda persona: el control de la información que le concierne. Que no consiste en una exquisitez jurídica ni

[13] Véase, Sentencia Tribunal Constitucional 292/2000 de 30 de Noviembre. FJ 7.
[14] GALAN MUÑOZ, A. *La protección jurídica de la intimidad y de los datos de carácter personal frente a las nuevas tecnologías de la información y comunicación.* Ed. Tirant lo Blanch, Valencia, 2014, p-211.

en un capricho, sino en una pretensión esencial en la sociedad en la que vivimos. Sin ese control, sin los límites que comporta para los poderes públicos y para los sujetos privados, ya sean los gobernantes, ya sean las empresas u otras entidades privadas, contarán no sólo con un conocimiento potencialmente pleno de la vida de cada uno de nosotros, sino que lo utilizarán para tomar decisiones que nos afectarán directa o indirectamente pero siempre de manera decisiva. El resultado será que estará en peligro el libre desenvolvimiento de nuestra vida e, incluso, nuestra propia identidad." [15]

Es por todo ello que el derecho a la protección de datos no es poca broma, ni debe considerarse un derecho fundamental de segunda clase. Es un derecho en consonancia con nuestra sociedad cada vez más tecnológica, más viral, más informática. Estamos viviendo en la edad de oro de las nuevas tecnologías por lo que debemos tener derechos que nos protejan ante ellas o ante quienes las usen de forma incorrecta o ilícita.

Todos los ordenadores tienen una IP que hace que podamos encontrar el ordenador en cuestión. En el caso de los humanos, nuestros datos son nuestra IP, es lo que nos hace reconocibles, nos crea un perfil determinado. Por lo tanto nuestros datos son una expresión de lo que somos cada uno de nosotros.

3. Concepto actual de derecho a la protección de datos y derechos ARCO.

Para poder dar una correcta y concreta definición del derecho a la protección de datos, acudimos de nuevo a la jurisprudencia del Tribunal Constitucional. Concretamente a dos, que están muy diferenciadas en el tiempo, lo que es positivo para poder comprobar cómo ha evolucionado el contenido del derecho.

- Sentencia Tribunal Constitucional 94/1998, de 4 de Mayo: *"La protección de datos es un derecho fundamental por el que se garantiza a la persona el control sobre sus datos, cualesquiera datos personales que se trate, y sobre su uso y destino, para evitar el tráfico ilícito de los mismos o lesivos para la dignidad y los derechos de los afectados. Se configura como un derecho del ciudadano para oponerse a que determinados datos personales sean usados para fines distintos a aquél que justificó su obtención."*

[15] MURILLO DE LA CUEVA, P.L: "Perspectivas del derecho a la autodeterminación informativa.", *Revista de Internet, Derecho y Politice*, número 5, 2007, p-30.

- Sentencia Tribunal Constitucional 39/2016, de 3 de Marzo: *"Consiste en el 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, ya sea el Estado o un particular, o cuales puede este tercero recabar, y que también permita al individuo saber quién puede usar esos datos personales y para qué, pudiendo oponerse a esa posesión o uso."*

En la sentencia de 1998 se fundamenta el derecho en garantizar al ciudadano el control sobre sus datos con la finalidad de evitar posibles daños o intromisiones ilegitimas. En cambio en la sentencia de 2016, además de ese precepto garantista se añaden los tradicionales derechos ARCO. Las siglas ARCO, significan lo siguiente:

- Acceso: permite al ciudadano conocer y obtener información sobre sus datos de carácter personal sometidos a tratamiento.[16]
- Rectificación: permite corregir informaciones inexactas o modificar datos incompletos.[17]
- Cancelación: permite suprimir determinados datos cuando resultan inadecuados o excesivos. [18]
- Oposición: el derecho a que no se lleve a cabo el tratamiento de éstos o se cese en el mismo cuando no sea necesario su consentimiento para el tratamiento, por la concurrencia de un motivo legítimo y fundado, referido a su concreta situación personal, que lo justifique, y siempre que una Ley no disponga lo contrario.[19]

Además de los tradicionales derechos ARCO, con el Reglamento General de Protección de Datos se han añadido varios nuevos derechos, como el derecho a la transparencia de información o el derecho de supresión (derecho al olvido).

---

[16]Véase,http://www.agpd.es/portalwebAGPD/CanalDelCiudadano/derechos/principales_derchos/acceso-ides-idphp.php

[17]Véase,http://www.agpd.es/portalwebAGPD/CanalDelCiudadano/derechos/principales_derchos/rectificacion-ides-idphp.php

[18]Véase,http://www.agpd.es/portalwebAGPD/CanalDelCiudadano/derechos/principales_derchos/cancelacion-ides-idphp.php

[19]Véase,http://www.agpd.es/portalwebAGPD/CanalDelCiudadano/derechos/principales_derchos/oposicion-ides-idphp.php

CAPÍTULO II. EL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS.

1. Introducción

Como punto de partida legislativo para el reconocimiento y desarrollo de la protección de datos destaca la Declaración Universal de Derechos Humanos : *"Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio, o su correspondencia, ni de ataques a su honra o su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques*[20]*."* La Declaración Universal de DDHH es del año 1948 cuando todavía no existía Internet, y el nacimiento de los ordenadores era algo novedoso. Pues el primer ordenador digital (Colossus) fue durante la II Guerra Mundial. Situándonos en este contexto histórico, es lógico que la referencia principal a la protección de datos sea a la correspondencia.

Dos años más tarde, el Convenio Europeo para la Protección de los Derechos Humanos y Libertades Fundamentales del Consejo de Europa 2 establece: *"Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.*[21]*"* De nuevo la protección de datos tiene una relación estrecha con la correspondencia y no con otros medios que en eso momento no existían o no eran alcanzables para la sociedad en general.

Se produce un salto temporal, y en el Convenio 108 del Consejo de Europa 3 en 1981 establece: *"(...) 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 correspondiente a dichas personas*[22]*."* El cambio es bastante apreciable, en treinta años se pasó de proteger la correspondencia a hablar ya de un tratamiento automatizado de los datos.

En 1995 se crea la Directiva 95/46/CE sobre la protección de datos personales, cuyo objetivo principal además de proteger los datos de los ciudadanos es conseguir que haya una libre circulación de datos, eliminando las posibles barreras existentes entre los Estados miembros.

---

[20] Declaración Universal de los Derechos Humanos, artículo 12.
[21] Convenio Europeo para la Protección de los Derechos Humanos y Libertades Fundamentales del Consejo de Europa 2, artículo 8.
[22] Convenio 108 del Consejo de Europa 3, artículo 1.

En esta línea, pero en el comienzo del siglo XX se proclama la Carta de Derechos Fundamentales de la UE, en cuyo artículo 8 se establece: "*Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan."* Y en el apartado segundo del mismo: *"Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación"* Ya no solo se habla de datos sino que además se añade el derecho a rectificar los mismos.

Veinte años más tarde entra en vigor el Reglamento General de Protección de Datos que deroga la Directiva que había regido ésta materia hasta la fecha. Su entrada en vigor fue en Mayo de 2016, pero no es hasta el 25 de Mayo de 2018 cuando ha sido de aplicación.

2. Objetivos del RGPD.

El Reglamento General de Protección de Datos (en adelante RGPD), ha supuesto la revisión de las bases legales sobre la materia establecidas en la Unión Europa. No se puede considerar al Reglamento como una actualización de la norma anterior, sino como una regulación que cambia el modelo europeo sobre protección de datos. Procediendo por un lado, a modernizar la normativa existente y por otro lado a unificar las legislaciones de los diferentes estados miembros.

Hasta ahora, el objeto de la regulación sobre protección de datos era la de garantizar y proteger las libertades públicas y los derechos fundamentales en relación con el tratamiento de datos de carácter personal. Pero el RGPD va un paso más adelante y sienta sus objetivos sobre tres pilares fundamentales:

1. La protección de Derechos Fundamentales y Libertades Públicas.
2. La libre circulación de datos personales en la UE: Debido a las incoherencias que surgían con la anterior directiva se dificultaba la libre circulación de datos en el mercado interior. Es por ello que con el actual Reglamento se intenta proporcionar seguridad jurídica y transparencia a los operadores económicos asi como a las microempresas y pequeñas y medianas empresas.
3. Armonizar la dispersión normativa existente: Los avances tecnológicos han transformado tanto la economía como la vida social, y estos avances requieren de un marco normativo más sólido; pues en muchos sentidos la legislación sobre protección de datos había quedado obsoleta. La principal razón de que éste sea uno de los objetivos del RGPD es porque hasta ahora con la Directiva 95/46/CE

se había producido una regulación fragmentada, pues la Directiva tuvo que ser traspuesta al derecho de cada Estado. Por lo tanto esto provocaba una inseguridad jurídica que era necesario subsanar. Es por todo esto que la nueva legislación va a ser equivalente en todos los Estados miembros (aunque el propio RGPD permite que determinadas normas sean especificadas o restringidas por el Derecho de los Estados Miembros para dotarlos de coherencia) para que el tratamiento de datos personales sea coherente y homogénea.

3. Ámbitos de aplicación material y territorial.

- Ámbito material.

El ámbito material del Reglamento General de Protección de Datos aparece regulado en su artículo 2. Además de los considerando 14-21, y 27. De tal forma que el RGPD se aplica al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero. Cuando la normativa específica un "tratamiento automatizado" se refiere a archivos o ficheros informáticos mientras que un "tratamiento no automatizado" son documentos en papel que no están informatizados. Sea como fuere, para ambos tipos de tratamientos es aplicable el Reglamento.

Ahora bien, no se aplicará a:

- Actividades no comprendidas en el ámbito de aplicación del Derecho de la Unión.
- Cuando se trate de actividades comprendidas en el ámbito de aplicación del Capítulo II del Título V del TUE. Es decir, cuando sean disposiciones especificas sobre política exterior y de seguridad común.
- Actividades exclusivamente personales o domésticas. El "considerando 18" aclara que materias están incluidas dentro de tales actividades siendo la correspondencia, así como la llevanza de un repertorio de direcciones, o las actividades en las redes sociales y la actividad en línea en el contexto de esas actividades personales y domesticas.
- A las autoridades competentes con fines de prevención, investigación, detección, o enjuiciamiento de infracciones penales, o de ejecuciones de sanciones penales.

- Ámbito territorial.

En el caso del ámbito territorial tenemos dos supuestos diferenciados:

- Cuando el establecimiento esté dentro de la Unión Europea: Establece el artículo 3 del RGPD que se aplicara al tratamiento de datos personales en el contexto de actividades de un establecimiento del responsable o del encargado en la Unión, independientemente de que el tratamiento tenga lugar dentro de la UE o no.
- Cuando sean ciudadanos o interesados residentes de la Unión Europea pero cuyo encargado del tratamiento no esté establecido en la Unión. Siempre y cuando las actividades estén relacionadas con la oferta de bienes o servicios a dichos interesados en la Unión, o, el control de su comportamiento en la medida en que éste tenga lugar dentro de la Unión.

4. Principios del Reglamento General de Protección de Datos.

En el artículo 5 se redactan los principios relativos al cumplimiento de ésta normativa siendo los siguientes:

- Principio de transparencia (articulo 5.1.a): El artículo establece "Los datos personales serán tratados de manera lícita, leal y transparente en relación con el interesado". Es necesario poner en relación dicho artículo con el "considerando 39" ya que fija la regla de que las personas físicas debemos saber que se están recogiendo o utilizando nuestros datos. Además de que toda información relativa al tratamiento de datos debe ser accesible y fácil de entender. La materialización del contenido de este principio supone el fin de la obligación de notificar y registrar los ficheros que contienen datos personales ante la autoridad de control. En España esa autoridad de control es la Agencia de Protección de Datos.
- Principio de limitación de la finalidad (articulo 5.1.b): "Los datos personales serán recogidos con fines determinados, explícitos, y legítimos, no serán tratados ulteriormente de manera incompatible con dichos fines." Estos fines serán determinados en el omento de recogida de datos.
- Principio de minimización de datos (articulo 5.1.c): "*Los datos personales serán adecuados, pertinentes, y limitados a lo necesario en relación con los fines para los que son tratados"*. Es decir, que se debe garantizar que solo serán objeto los

datos personales necesarios. [23] En esta línea el considerando 39 añade que "*Los datos personales deben tratarse si la finalidad del tratamiento no pudiera lograrse de forma razonada a través de otros medios."*

- Principio de exactitud (artículo 5.1.d): "*Exactos y, si fuera necesario actualizados*" Se exige al responsable del tratamiento que actúe con la diligencia necesario para asegurar que los datos que son objeto del tratamiento son correctos y que están actualizados. Este principio está directamente relacionado con el derecho de rectificación (articulo 16 RGPD) de tal forma que si el usuario detecta alguna inexactitud puede solicitar la modificación de esos datos a través de una petición que deberá ser atendida en el plazo de un mes por el responsable.
- Principio de limitación de plazo (articulo 5.1.e): "*Mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales."* Estipula qe los datos solo deberán conservarse durante el tiempo estrictamente necesario para los alcanzar los fines del tratamiento. A excepción de cuando se trate de archivos de interés público, o sean con fines de investigación científica, histórica o estadística. Además entra la información que se le debe aportar al interesado se incluye el plazo de conservación o al menos los criterios utilizados para determinarlo.
- Principio de integridad y confidencialidad (articulo 5.1.f): *"Tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su perdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas.*" En definitiva responsable y encargado del tratamiento deberán analizar y evaluar los riesgos propios del tratamiento y aplicar medidas para disminuir esos riesgos. Así que deberán llevarse a cabo medidas que garanticen la seguridad y confidencialidad de los datos para poder impedir un posible acceso no autorizado.
- Principio de responsabilidad proactiva (art 5.2): "*El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo."* Así, a través de este principio, el responsable y encargado del tratamiento estarán obligados a demostrar que la forma en la que han

[23] Artículo 25.2 del Reglamento General de Protección de Datos.

desarrollado el tratamiento es la forma adecuada para el cumplimiento de éstos principios. Para ello se deberán implantar medidas apropiadas cuyo objetivo final sea el de demostrar que el tratamiento realizado es adecuado al RGPD, éstas medidas además deberán ir actualizándose. Las principales medidas serían las siguientes:

- *Registro de actividades.*
- *Medidas de Proteccion de Datos desde el diseño.*
- *Medidas de Protección de Datos por defecto.*
- *Medidas de Seguridad Adecuadas.*
- *Evaluaciones de Impacto.*
- *Autorización previa.*
- *Delegado de Protección de Datos.*
- *Notificación de Violación de Seguridad.*

5. ¿Qué debe hacer una empresa para cumplir con el RGPD?

Lo primero que se debe resolver respecto de esta vertiente es, ¿a qué empresas afecta el Reglamento General de Protección de Datos? La respuesta es que afecta a todas aquellas que guarden algún tipo de dato sobre ciudadanos de un país de la Unión Europea. Dos puntos son necesarios de clarificar:

1. No afecta a autónomos cuyo tratamiento de datos se limita a los trabajadores de la propia empresa.[24]
2. Afectará a aquellas empresas que traten datos de terceros de la Unión Europea aunque la propia empresa no esté establecida dentro de la Unión Europea. [25]

La Agencia Española de Protección de Datos puntualiza “siempre que realicen tratamiento de datos derivados de una oferta de bienes o servicios destinados a ciudadanos de la Unión Europea o como consecuencia de su motorización y seguimiento de su comportamiento.”

[24] Artículo 2 apartado c del Reglamento General de Protección de Datos.

[25] Artículo 3.1 del Reglamento General de Protección de Datos.

Para facilitar estos cambios a las empresas, la Agencia Española de Protección de Datos ha elaborado lo que ellos han denominado "hoja de ruta" sobre cómo adaptarse al RGPD. Esos pasos son los siguientes:[26]

1. Designar un Delegado de Protección de Datos. Tanto si es obligatorio para la empresa como si no, es recomendable que de forma voluntaria identifique a una persona responsable de coordinar la adaptación.
2. Elaborar un registro de actividades de tratamiento.
3. Realizar un análisis de riesgos. La gestión o análisis de riesgos se centra fundamentalmente en tres pasos:[27]
    a) Identificar las amenazas. Éstas amenazas pueden ser de tres tipos:
        - Acceso ilegal a los datos.
        - Modificación no autorizada de los datos.
        - Eliminación de los datos.
    b) Evaluar los riesgos. Consiste en valorar el impacto de la exposición de la amenaza junto con la probabilidad de que ésta se materialice.
    c) Tratar los riesgos. Consiste en disminuir la exposición de los datos con medidas de control que permiten reducir la probabilidad de que estos se materialicen.
4. Revisar las medidas de seguridad en base a los resultados del análisis de riegos.
5. Establecer mecanismos y procedimientos de notificación de quiebras de seguridad.
6. A partir de los resultados del análisis/gestión de riesgos, realizar, en su caso una evaluación de impacto en la protección de datos (de aquí en adelante EIPD). La EIPD es una herramienta que permite evaluar de manera anticipada cuáles son los principales riesgos a los que están expuestos los datos de carácter personal, en función de las actividades de tratamiento que se llevan a cabo con los mismos. En definitiva, permite determinar el nivel o el grado de riesgo que entraña un determinado tratamiento, con el objetivo de establecer medidas de control que sean más adecuadas. Y de esa forma reducir el riesgo. La EIPD está dividida en las siguientes fases:

[26]http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/infografias/Adaptacion_RGPD_sector_privado.pdf.
[27]http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/2018/AnalisisDeRiesgosRGPD.pdf

I. Describir el ciclo de vida de los datos. Ese ciclo es el siguiente:
   - Captura de datos: Consiste en el proceso que se lleva a cabo para obtener los datos.
   - Clasificación/Almacenamiento: Establecer categorías y asignarlas a los datos para su clasificación y almacenamiento dentro de los sistemas o archivos.
   - Uso/Tratamiento: Operaciones que se hayan realizado sobre los datos personales.
   - Cesión o transferencia de los datos a un tercero para su tratamiento.
   - Destrucción: Eliminar los datos que puedan estar contenidos en los sistemas o archivos, de tal forma que no puedan ser recuperados.

II. Analizar la necesidad y proporcionalidad del tratamiento.

III. Identificar amenazas.

IV. Evaluar los riesgos.

V. Tratar los riesgos.

VI. Plan de acción y conclusiones. Consiste en un informe de conclusiones de la EIPD donde se documenta el resultado obtenido junto con el plan d acción que incluyen las medidas de control a implantar.

La EIPD deberá actualizarse cuando se produzca una variación relevante en el contexto de las actividades que puedan suponer un aumento del riesgo para los datos.[28]

Además de todo lo anterior se deberá realizar de forma simultánea lo siguiente:

- Adecuar los formularios.
- Adaptar los mecanismos y procedimientos para el ejercicio de los derechos.
- Valorar si los encargados ofrecen garantías y adaptación de contratos.
- Elaborar / adaptar políticas de privacidad.

[28]Véase,http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/2018/Guia_EvaluacionesImpacto.pdf

6. Delegado de Protección de Datos.

A partir de la entrada en vigor del Reglamento General de Protección de Datos el 25 de Mayo, la figura del Delegado De Protección de Datos (en adelante DPD), será el elemento central para el cumplimiento del nuevo marco jurídico de protección de datos.

El DPD será obligatorio en algunos supuestos, y voluntario para el resto. El Grupo de Trabajo 29 ha alentado a que las empresas no obligadas designen a una persona para llevar a cabo esas funciones.

Aunque esta figura pueda parecer novedosa, no lo es. Sí es cierto que no aparecía en la Directiva 95/46/CE pero es un elemento que está implementado desde hace años en algunos países.

La figura del Delegado de Protección de Datos será obligatoria en los siguientes supuestos:[29]

- Si el tratamiento lo lleva a cabo una autoridad u organización pública.
- Si las actividades principales del responsable o encargado consisten en operaciones de tratamiento que, en razón de su naturaleza, alcance o fines, requieren una observación habitual y sistemática de interés a gran escala.
- Si las actividades principales del responsable o encargado consisten en el tratamiento a gran escala de categorías especiales de datos personales o de datos relativos a condenas e infracciones penales.

Para comprender los supuestos es necesario definir palabras claves:[30]

Las actividades principales a las que se refiere el artículo 37.1 son las operaciones claves para lograr el objetivo del responsable. Por ejemplo: el tratamiento de datos relativos a la salud, como pueden ser los historiales de los pacientes, debe considerarse una de las actividades principales de un hospital y por ende, los hospitales deben designar a un DPD.

[29] Véase artículo 37.1 del Reglamento General de Protección de Datos

[30] http://www.agpd.es/portalwebAGPD/canaldocumentacion/docu_grupo_trabajo/wp29/common/Traduc_oficial_ult_version/wp243revol_es.pdf

A la hora de determinar si el tratamiento se realiza a gran escala se siguen las siguientes directrices:

- El número de interesados afectados.
- El volumen de datos.
- La duración de la actividad.
- El alcance geográfico de la actividad.

Siguiendo estos parámetros son tratamientos a gran escala, por ejemplo: el tratamiento de datos de clientes llevado a cabo por una compañía de seguros o entidad bancaria. También es tratamiento a gran escala el desarrollado por proveedores de telefonía o internet.

Por el contrario, no son tratamiento a gran escala, por ejemplo: el tratamiento de datos de pacientes por un solo médico. Tampoco lo sería el tratamiento de datos relativos a condenas e infracciones penales por parte de un abogado.

Y en cuanto a la noción de observación habitual y sistemática hay que atender a lo que señala el considerando 24 del RGPD: ”*Para determinar si se puede considerar que una actividad de tratamiento controla el comportamiento de los interesados, debe evaluarse si las personas físicas son objeto de un seguimiento en internet, inclusive el potencial uso posterior de técnicas de tratamiento de datos personales que consistan en la elaboración de un perfil de una persona física con el fin, en particular, de adoptar decisiones sobre él o de analizar o predecir sus preferencias personales, comportamientos y actitudes.”* Incluye toda forma de seguimiento y creación de perfiles en internet, también con fines de publicidad.

Por lo tanto, esto es lo que describe el RGPD como supuestos en los que debe haber un DPD. Éstas definiciones fueron muy criticadas en su momentos porque en lugar de aclarar, sembraban nuevas dudas. Respecto a esta materia los Estados han tenido competencias para perfilar los supuestos, y el Proyecto de Ley Orgánica de Protección de Datos, ha establecido los siguientes casos:[31]

1. Colegios profesionales y consejos generales.
2. Centros docentes y universidades públicas o privadas.

[31] Véase artículo artículo 34.1 del Proyecto de Ley Orgánica de Protección de Datos.

3. Entidades que exploten redes y presten servicios de telecomunicaciones.
4. Los prestadores de servicios de la sociedad de la información cuando elaboren datos a gran escala.
5. Las entidades de ordenación, supervisión y solvencia de entidades de crédito.
6. Establecimientos financieros.
7. Entidades aseguradoras y reaseguradoras.
8. Empresas de servicios de inversión.
9. Distribuidoras y comercializadoras de energía eléctrica.
10. 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.
11. Las entidades que desarrollen actividades de publicidad y prospección comercial.
12. Los centros sanitarios legalmente obligados al mantenimiento de las historias clínicas de los pacientes.
13. Las entidades que tengan como uno de sus objetos la emisión de informes comerciales que puedan referirse a personas físicas
14. Los operadores que desarrollen la actividad de juego a través de canales electrónicos, informáticos, telemáticos e interactivos
15. Quienes desempeñen las actividades reguladas por el Título II de la Ley 5/2014, de 4 de abril, de Seguridad Privada.

CAPITULO III. PROYECTO DE LEY ORGÁNICA DE PROTECCIÓN DE DATOS.

1. Evolución legislativa.

Nuestra Constitución de 1978 fue pionera en el reconocimiento de la protección de datos como Derecho Fundamental. Regulado de esa forma en el articulo 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.)*[32]

Tras este reconocimiento, fue necesaria regular la protección de datos mediante una ley orgánica. Surgiendo de esta forma la LO 5/1992, de 29 de Octubre, conocida como LORTAD. Es necesario poner de manifiesto el periodo temporal que transcurre desde que se reconoce como DDFF hasta que se promulga la ley orgánica necesaria para una protección efectiva. La razón es que con anterioridad la protección de datos se consideraba protegida por el ámbito de aplicación de las leyes que regulaban los derechos a la personalidad. Pero una vez adentrados en los años 90 empiezan el auge de las nuevas tecnologías y con ello un potencial peligro de menoscabar el derecho a la protección de datos. "*Las modernas técnicas de comunicación permiten salvar sin dificultades el espacio, y la informática posibilita almacenar todos los datos que se obtienen a través de las comunicaciones y acceder a ellos en apenas segundos, por distante que fuera el lugar donde transcurrieron los hechos, o remotos que fueran éstos*."[33]

La LORTAD estaba divida en una parte general y otra parte especial. Esa primera parte general estaba compuesta por un conjunto de principios cuyo objetivo era el uso eficiente de los datos de los ciudadanos y su protección. Lo que se pretendía era darles garantías a los ciudadanos a través de una seria de derechos, especialmente, los derechos de autodeterminación, amparo, rectificación y cancelación. Siendo todos ellos el eje central de la Ley, es decir, que éstos eran los mecanismos que desarrollaban el sistema cautelar o preventivo instaurado.

Uno de los hitos más importantes de la LORTAD es que creó un órgano independiente para controlar la eficacia de las disposiciones desarrolladas en dicha ley. Este órgano,

[32] Constitución Española de 1978, artículo 18.4.
[33] Exposición de Motivos de la Ley Orgánica 5/1992, LORTAD.

vigente hoy día y de enorme importancia, es la Agencia Española de Protección de Datos.

La LORTAD fue reemplazada por la LO 15/1999, de 13 Diciembre que nació con motivo de la transposición a nuestro Derecho de la Directiva 95/46/CE del Parlamento Europeo y el Consejo. La razón de esta Directiva fue la necesidad de armonizar legislaciones dentro de la Unión Europea, debido en gran medida a dos cuestiones. En primer lugar el avance que habían supuesto las nuevas tecnologías en los últimos años, que conllevaba una puesta en peligro cada vez mayor para los ciudadanos y el tratamiento de sus datos. Y en segundo lugar por acabar con legislaciones tan diferentes sobre un mismo tema dentro de un mismo territorio como es la Unión Europea.

Alguno de los factores que impulsaron la creación de esta Directiva en relación a la protección de datos son los siguientes:

- Factores relativos al mercado interior. Debido a la libre circulación de mercancías, personas, servicios y capitales, también se produce una circulación o intercambio de datos. Lo que provoca que sea necesario proteger los DDFF que puedan verse vulnerados por éstas actividades.
- Factores relativos a la actividad económica y social. En base al avance y alcance de las nuevas tecnologías, mediante las actividades económicas (desde un punto de vista laboral, empresarial o personal) y las sociales dejamos un rastro de datos que es necesario proteger.
- Factores relativos a la cooperación científica y técnica, nuevas redes de telecomunicación en la UE. Todo ello exige y facilita la circulación transfronteriza de datos personales.
- Factores relativos a la aproximación de legislaciones.

Con posterioridad a la entrada en vigor de la LO 15/1999, se lleva a cabo el Real Decreto 1720/2007 por el que se aprueba el Reglamento de desarrollo de la LO 15/1999 (RLOPD). Este Reglamento nace con la finalidad, no de reiterar conceptos expuestos en la LOPD, sino de desarrollar otros que en la LOPD solo se mencionan o se prevén características generales y necesitan de un desarrollo normativo. Por lo tanto el principal objetivo del RLOPD es dar coherencia a la transposición de la directiva y además

perfeccionar ciertos aspectos novedosos introducidos por la ley orgánica y que necesitan de una mayor legislación.

La LOPD así como su Reglamento de Desarrollo relativo han estado vigentes hasta la actualidad. El motivo del cambio legislativo vuelve a ser una norma proveniente de la UE, esta vez un Reglamento, concretamente el Reglamento General de Protección de Datos.

Situándonos en el contexto, y en el periodo de años que ha transcurrido desde 1999 (anterior ley) hasta la actualidad (2018, y en el caso de la creación del Reglamento 2017) han sido más de quince años, en los que la revolución tecnológica ha cambiado todo a nuestro alrededor. Desde nuestro ámbito laboral hasta una esfera más privada todo ha sido modificado, y nuestros datos son ahora mucho más vulnerables que a principios de siglo. Por lo tanto era un escenario en el que se dibujaba cada vez más necesario una nueva legislación que abordara los nuevos retos a los que nos enfrentamos.

La UE dio respuesta a todas las dudas que estaban surgiendo alrededor de la protección de datos con el Reglamento General de Protección de Datos. El Reglamento es de aplicación directa pero necesitan, por lo general, de leyes internas de cada país para complementarlo y/o desarrollarlo. Siguiendo este camino, era necesario derogar la ley 15/1999, para dar lugar a una ley que estuviera en concordancia con las nuevas estipulaciones de la UE.

Por estas razones y por motivos de seguridad jurídica, se ha procedido a elaborar una norma que permita la correcta adaptación del nuevo RGPD a nuestro sistema español.

Este Proyecto de LOPD fue presentado el 24 de Noviembre de 2017, y se va a analizar a continuación.

2. Proyecto de Ley Orgánica de Protección de Datos: Objeto y estructura.

- Objeto

En referencia al objeto de esta LOPD es básicamente la adopción del ordenamiento jurídico español al nuevo Reglamento General de Protección de Datos y además completar sus disposiciones. Así aparece configurado en dicha ley cuando establece: "*1. La presente ley orgánica tiene por objeto adaptar el ordenamiento jurídico español*

al Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos, y completar sus disposiciones."[34]

- Estructura

Este proyecto de LO de Protección de Datos estaría configurado de la siguiente forma:

- 78 artículos.
- 8 Títulos:

  - Título I. Disposiciones Generales.
  - Título II. Principios de Protección de Datos.
  - Título III. Derechos de las personas
  - Título IV. Disposiciones aplicables a tratamientos concretos.
  - Título V. Responsable y encargado del tratamiento
  - Título VI. Transferencias internacionales de datos.
  - Título VII. Autoridades de Protección de Datos.
  - Título VIII. Procedimiento en caso de posible vulneración de la normativa de Protección de Datos.

- 10 Disposiciones Adicionales
- 5 Disposiciones transitorias
- 1 Disposición derogatoria
- 7 Disposiciones Finales

3. Principales novedades del Proyecto de Ley Orgánica de Protección de Datos en relación con la antigua legislación.

El Proyecto de Ley Orgánica de Protección de Datos introduce numerosas novedades impulsadas, en gran medida, por el RGPD de la UE. Las principales novedades en atención a la legislación anterior serían las siguientes:

[34] Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal. Articulo 1.1

- Se excluye del ámbito de aplicación de la ley a las personas fallecidas. Pero se permite que los herederos puedan solicitar el acceso a los datos, así como llevar a cabo el ejercicio de rectificación o supresión. Con la excepción de que la persona fallecida lo hubiera prohibido expresamente o así fuera establecido en la ley. Regulación en el articulo 2.d en relación con el artículo 3:

  "Articulo 2. Esta ley orgánica no será de aplicación: d) A los tratamientos de datos de personas fallecidas, sin perjuicio de lo establecido en el artículo."[35]

  "Artículo 3. Datos de las personas fallecidas. 1. Los herederos de una persona fallecida que acrediten tal condición mediante cualquier medio válido conforme a Derecho, podrán dirigirse al responsable o encargado del tratamiento al objeto de solicitar el acceso a los datos personales de aquella y, en su caso, su rectificación o supresión. Como excepción, los herederos no podrán acceder a los datos del causante, ni solicitar su rectificación o supresión, cuando la persona fallecida lo hubiese prohibido expresamente o así lo establezca una ley."[36]

- La persona en cuestión deberá dar su consentimiento expreso. No será válido el consentimiento tácito.

  "Artículo 6. Tratamiento basado en el consentimiento del afectado. 1. De conformidad con lo dispuesto en el artículo 4.11 del Reglamento (UE) 2016/679, se entiende por consentimiento del afectado toda manifestación de voluntad libre, específica, informada e inequívoca por la que éste acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen. 2. Cuando se pretenda fundar el tratamiento de los datos en el consentimiento del afectado para una pluralidad de finalidades será preciso que conste de manera específica e inequívoca que dicho consentimiento se otorga para cada una de ellas. 3. No podrá supeditarse la ejecución del contrato a que el afectado consienta el tratamiento de los datos personales para finalidades que no guarden relación con el mantenimiento, desarrollo o control de la relación contractual."[37]

- Se fija la edad en la que los menores podrán otorgar su consentimiento. Ésta es una de las materias en las que se permite que cada país decida. El RGPD

[35]Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal. Artículo 2.d).
[36] Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal. Artículo 3.
[37] Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal. Artículo 6.

establece la edad mínima en 14 años pero en España no se mantiene esta edad. Será la edad de 13 años, adecuando así nuestra legislación a la del resto de países de nuestro entorno.

"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 trece años"[38].

- La figura del Delegado de Protección de Datos (DPO/DPD). Esta figura es tal vez la principal novedad introducida por el RGPD, pero el Reglamento solo lo conceptúa y no establece en que supuestos debe desarrollarse sus funciones. Pero el Proyecto de LO de Protección de Datos sí establece éstos supuestos en su artículo 34.1:

  "a) Los colegios profesionales y sus consejos generales, regulados por la Ley 2/1974, de 13 febrero, sobre colegios profesionales.

  b) Los centros docentes que ofrezcan enseñanzas reguladas por la Ley Orgánica 2/2006, de 3 de mayo, de Educación, y las Universidades públicas y privadas

  c) Las entidades que exploten redes y presten servicios de comunicaciones electrónicas conforme a lo dispuesto en la Ley 9/2014, de 9 de mayo, General de telecomunicaciones, cuando traten habitual y sistemáticamente datos personales a gran escala.

  d) Los prestadores de servicios de la sociedad de la información cuando elaboren a gran escala perfiles de los usuarios del servicio.

  e) Las entidades incluidas en el artículo 1 de la Ley 10/2014, de 26 de junio, de ordenación, supervisión y solvencia de entidades de crédito.

  f) Los establecimientos financieros de crédito regulados por Título II de la Ley 5/2015, de 27 de abril, de fomento de la financiación empresarial.

  g) Las entidades aseguradoras y reaseguradoras sometidas a la Ley 20/2015, de 14 de julio, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras.

[38] Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal. Artículo 7.

h) Las empresas de servicios de inversión, reguladas por el Título V del texto refundido de la Ley del Mercado de Valores, aprobado por Real Decreto Legislativo 4/2015, de 23 de octubre.

i) Los distribuidores y comercializadores de energía eléctrica, conforme a lo dispuesto en la Ley 24/2013, de 26 de diciembre, del sector eléctrico, y los distribuidores y comercializadores de gas natural, conforme a la Ley 34/1998, de 7 de octubre, del sector de hidrocarburos.

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 el artículo 32 de la Ley 10/2010, de 28 de abril, 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.

l) Los centros sanitarios legalmente obligados al mantenimiento de las historias clínicas de los pacientes con arreglo a lo dispuesto en la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.

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 lo dispuesto en la Ley 3/2011, de 27 de mayo, de regulación del juego.

ñ) Quienes desempeñen las actividades reguladas por el Título II de la Ley 5/2014, de 4 de abril, de Seguridad Privada."[39]

Además en el apartado segundo de dicho artículo se establece la posibilidad de que las empresas o entidades no mencionadas designen de forma voluntaria a un delegado de protección de datos.

[39] Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal. Artículo 34.1.

- Las cámaras de video vigilancia podrán captar la vía pública siempre y cuando el objeto sea preservar la seguridad de las personas y los bienes de la empresa.

"Artículo 22. Tratamientos con fines de video vigilancia. 1. Las personas físicas o jurídicas, públicas o privadas, podrán llevar a cabo el tratamiento de imágenes a través de sistemas de cámaras o videocámaras con la finalidad de preservar la seguridad de las personas y bienes, así como de sus instalaciones. 2. Sólo podrán captarse imágenes de la vía pública en la medida en que resulte."[40]

4. Principales diferencias entre la LOPD y el RGPD.

- Respecto del consentimiento:

En la LOPD se establece que el consentimiento debe ser inequívoco, siempre y cuando no se trate de datos especialmente sensibles.[41] Mientras que en la nueva regulación europea se exige un consentimiento libre, informado, específico e inequívoco. Para que sea considerado inequívoco deberá existir una declaración del interesado o una acción positiva, de tal forma que el silencio, las casillas marcadas o la inacción no constituyen prueba del consentimiento.[42]

En el Proyecto de Ley Orgánica de Protección de Datos, se hace referencia a la exclusión del consentimiento tácito y además está regulado en los mismos términos del RGPD en el artículo 6.

Se recomienda a las empresas que revisen la forma en la que recogen el consentimiento y eliminen las prácticas que eran acordes a la ya antigua legislación pero que son ilícitas con el Reglamento.

- Respecto de los nuevos derechos.

En la LOPD se recogían los tradicionales "derechos ARCO", relativos al derecho de acceso, de rectificación, de cancelación y de oposición. Pero el RGPD ha ido un paso más allá y ha recogido cuatro nuevos derechos necesarios y acordes a la Era Tecnológica que estamos viviendo. Éstos nuevos derechos son los siguientes:

[40] Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal. Artículo 22.
[41] Proyecto de Ley Orgánica Protección de Datos de Carácter Personal. Artículo 6.
[42] Reglamento General de Protección de Datos, considerando 32.

- Derecho a la transparencia de información: Este derecho establece que cuando los datos sean obtenidos bien a través de redes de comunicaciones electrónicas o bien otros supuestos expresamente tasados, o autorizado por la AEPD, el responsable del tratamiento deberá facilitar al afectado una "información básica". Ésta información básica consiste en: la identidad del responsable del tramiento y en su caso, de su representante. La finalidad del tratamiento y el modo en el que podrán ejercitarse los derechos del art 15 al 22 del RGPD.

  También se puede dar el caso de que los datos no hubiesen sido obtenidos de forma directa, de tal forma, que el responsable también deberá hacerle llegar esa "información básica" que en este supuesto consistirá en las categorías de datos objeto del tratamiento y las fuentes de las que procede la información. [43]
- Derecho al olvido: No es un derecho autónomo sino una consecuencia de la ejecución del derecho de cancelación. Por lo tanto es una manifestación del derecho de cancelación u oposición en el entorno online[44]. Consiste en el derecho de los ciudadanos a solicitar la eliminación de información que esté expuesta en Internet, siempre atendiendo a unos criterios.
- Derecho de limitación: Consiste en el derecho de no aplicar a los datos personales un determinado tratamiento. *Se puede solicitar la limitación cuando*:

- El interesado ha ejercido los derechos de rectificación u oposición y el responsable está en proceso de determinar si procede atender a la solicitud.
- El tratamiento es ilícito, lo que determinaría el borrado de los datos, pero el interesado se opone a ello.
- Los datos ya no son necesarios para el tratamiento, que también determinaría su borrado, pero el interesado solicita la limitación porque los necesita para la formulación, el ejercicio o la defensa de reclamaciones.[45]

- Derecho de portabilidad: El derecho a la portabilidad implica que los datos personales del interesado se transmiten directamente *de un responsable a otro*,

[43]Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal. Artículo 11.
[44] Guía del Reglamento General de Protección de Datos para Responsable del Tratamiento. Página 10. https://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/guia_rgpd.pdf.
[45] Guía del Reglamento General de Protección de Datos para Responsable del Tratamiento. Página 11. https://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/guia_rgpd.pdf.

sin necesidad de que sean transmitidos previamente al propio interesado, siempre que ello sea técnicamente posible.[46]

Estos nuevos derechos, se encuentran a sí mismo, en el Proyecto de LOPD. No son definidos, pues para ello te remite al RGPD pero sí que son desarrolladas determinadas cuestiones. El derecho a la transparencia de la información aparece recogido de forma separada del resto en el Capítulo I del Título III. Mientras que los otros; derecho al olvido (derecho de supresión), derecho de limitación y derecho de portabilidad están en el Capítulo II del Título II, en los artículos 15, 16 y 17 respectivamente.

- Respecto de la Evaluación de Impacto del Tratamiento de Datos Personales.

Uno de los pilares básicos del RGPD es la responsabilidad proactiva, es decir, las medidas que se deben llevar a cabo para evitar el daño de los datos. Una de las principales medidas es la Evaluación de Impacto del Tratamiento de Datos Personales, la cual ni siquiera existía en nuestra anterior legislación (LOPD). Estas EIPD son obligatorias cuando existe un alto riesgo para los derechos y libertades de las personas físicas, en la que se evalúe el origen, la naturaleza, la particularidad y la gravedad de dicho riesgo[47]

La evaluación de impacto es citada en el Proyecto de LOPD pero, para una vez más, remitir al RGPD.

- Respecto de la comunicación de los fallos a la autoridad.

No se regulaba en la LOPD. En cambio en la nueva regulación es uno de las principales bases. Consiste en la obligación, por parte del responsable del tratamiento, de informar a la autoridad competente (AEPD) cuando se produzca una brecha en la seguridad, además tendrá un plazo de 72 horas para hacerlo. Pero el RGPD no se queda ahí, sino que además también será necesario comunicárselo al interesado cuando el fallo pueda producir un grave riesgo para los derechos y libertades de la persona física. [48]

[46] Guía del Reglamento General de Protección de Datos para Responsable del Tratamiento. Página 12. https://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/guia_rgpd.pdf.
[47] Reglamento General de Protección de Datos, considerando 84.
[48] Reglamento General de Protección de Datos, articulo 34.

CAPITULO IV. DERECHO AL OLVIDO.

1. APROXIMACIÓN AL CONCEPTO.

Muchos autores lo tienen claro. "El derecho al olvido no existe".[49] Pero es necesario profundizar en la materia. Desde los años 80, cuando se adoptó la palabra Internet para definir una red de comunicación hasta la actualidad donde el intercambio de datos entra dentro de nuestra rutina y además es un intercambio global, han pasado cuatro décadas donde se ha puesto de manifiesto el peligro que puede generar la utilización indiscriminada de nuestros datos personales poniendo en jaque nuestra dignidad. Es por esto que es necesario el derecho al olvido. Y que debe de existir, para protegernos.

"El flujo masivo de la información personal en Internet obliga a evitar la banalización de las amenazas que genera en el individuo e invita a reforzar la vigencia del Derecho Fundamental a la protección de datos"[50]

Actualmente muchos ciudadanos tienden a compartir información personal en Internet, lo que provoca la creación de un determinado perfil, lo que conlleva:

1. Arriesgar nuestra privacidad.
2. Amenaza nuestra reputación, libertad y dignidad.

En este sentido, diferentes encuestas realizadas a lo largo de 2017, aseguraban que el 86% de las empresas utilizan Facebook para ver el perfil de la persona a la que van a contratar. [51] De tal forma que nosotros mismos estamos creando con la distribución de nuestros datos un perfil en Internet que no se tiene porque corresponder con la realidad, o en cualquier caso, deberíamos tener el derecho de poder suprimir esos datos en todo momento. Porque son susceptibles de ser utilizados por empresas contratantes, así como otras empresas de publicidad.

En conclusión, en el Universo de Internet pueden existir millones de datos de carácter personal sobre nosotros que se han ido almacenando con el paso del tiempo. Y no poder

---

[49] Rallo Lombarte, A.: *El derecho al olvido. Google versus España*, Ed. Centro de Estudios Politicos y Constitucionales

[50] Guerrero Pico, M.C: "*El impacto de Internet en el DDFF a la protección de datos de Carácter Personal*, Ed. Thomson Civitas, Pamplona, 2006.

[51] V Informe 2016 Infoempleo – Adecco sobre Redes Sociales y Mercado de Trabajo.

acabar con ellos, no poder borrarlos supone un atentado contra nuestra libertad individual.

Si tenemos libertad, debemos tener derecho al olvido.

La primera sentencia en España que reconoce el derecho al olvido es de una fecha muy reciente. Concretamente 2015. "Si los interesados lo solicitan, la información obsoleta sobre personas sin relevancia pública y careciendo de interés histórico que la información aparezca vinculada a dichas personas cuando se hace una búsqueda genera en Internet utilizando como palabras claves sus nombres y apellidos, el daño es tan desproporcionado que no resulta amparado por el ejercicio de la libertad de información."

Se puede definir el derecho al olvido como "el derecho que tiene el titular de un dato personal a borrar, bloquear, o suprimir información personal que considere obsoleta por el transcurso del tiempo o que de alguna manera afecte al libre desarrollo de sus Derechos Fundamentales."[52]

2. El olvido en la Unión Europea.

La primera referencia que se hizo al derecho al olvido fue realizada por Viviane Reding: "Los usuarios de Internet deben tener un control efectivo sobre lo que suben online y ser capaces de corregir, retirar y suprimir. Necesitamos aproximarnos al derecho al olvido." [53]

Estas palabras fueron pronunciadas en un lejano (temporal y tecnológicamente) 2010. Unos meses después de estas declaraciones, la Comisión Europea presentó en Bruselas el 4 de Noviembre de 2010 la Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social europeo y al Comité de las Regiones sobre un "enfoque global de la protección de datos personales en la Unión Europea". Se tomó como ejemplo las redes sociales (fenómeno incipiente en aquella época y que todavía no había explotado de la forma en la que lo conocemos hoy día), y es que son éstas una de

[52] ANÓNIMO: "Pero, ¿qué es el derecho al olvido en Internet?", ABC, Edición Digital, 14 de Mayo de 2014, 18:35 hrs, http://www.abc.es/tecnologia/redes/20140514/abci-derecho-olvido-google-sentencia-201405141455.html

[53] "Building Trust in Europe's Online Single Market", Speech at the American Chamber Of Commerce to the EU, Brussels, 22 June 2010.

las principales amenazas para nuestros datos y su efectiva protección. Se estipuló la necesidad de llevar a cabo un control basado en 4 puntos:

1. Reforzar el principio de minimización de datos.
2. Mejorar las condiciones para poder desarrollar un verdadero y efectivo ejercicio de los derechos de acceso, rectificación, supresión y bloqueo.
3. Garantizar la portabilidad de datos.
4. Clarificar el denominado derecho al olvido, como derecho de las personas a que sus datos dejen de utilizarse, y se supriman cuando ya no sean necesarios.

En un principio se orientó el derecho al olvido como un derecho basado en la cancelación de datos.

Para la AGPD la cancelación es el procedimiento en virtud del cual el responsable cesa en el uso de los datos. La cancelación implica el bloqueo de los datos, consistente en la identificación y reserva de los mismos con el fin de impedir su tratamiento excepto para su puesta a disposición de las Administraciones Públicas, Jueces y Tribunales, para la obtención de las posibles responsabilidades nacidas del tratamiento y solo durante el plazo de prescripción de dichas responsabilidades. Transcurrido ese plazo deberá procederse a la supresión de datos.

La AGPD también definió el derecho al olvido como "el derecho de impedir la difusión de información personal a través de Internet cuando su publicación no cumpla los requisitos de adecuación y pertinencia prevista en la normativa."

Siguiendo esta línea la **SENTENCIA DE LA AUDIENCIA NACIONAL DE 29 DICIEMBRE DE 2014** (recurso número 725/2010) establece: "*quién ejercite el derecho de oposición ha de indicar ante el responsable del tratamiento o ante la AEPD que la búsqueda se ha realizado a partir de su nombre, como persona física, indicar los resultados o enlaces obtenidos a través del buscador, así como el contenido de esa información que le afecta y que constituye un tratamiento de sus datos personales a la que se accede a través de dichos enlaces. La cancelación de esos datos estará justificada cuando las circunstancias de cada caso concreto así lo determinen, ya sea por la naturaleza de la información, su carácter sensible para la vida privada del afectado, por la no necesidad de los datos en relación con los fines para los que se recogieron o por el tiempo transcurrido, entre otras razones."*

En Noviembre de 2014, el grupo de trabajo de la UE sobre privacidad (GT29) pidió a Google, y al resto de buscadores, que el derecho al olvido fuese aplicado a nivel global, no solo a nivel de la Unión Europea. Concretamente el comunicado establecía lo siguiente:

Las decisiones que deben ser excluidas del listado (de búsqueda) deben ser aplicadas de tal manera que se garantice una protección efectiva y completa de los derechos del sujeto.

En este sentido, limitar la exclusión (de los resultados de búsqueda) a los dominios europeos no puede considerarse como un medio suficiente para garantizar de manera satisfactoria los derechos de los interesados.

En la práctica, esto significa que, en cualquier caso, la exclusión tiene que ser también efectiva en todos los dominios '.com' relevantes.

La respuesta del gigante Google fue tajante. "El derecho al olvido es solo cosa de Europa". Lo que provocaba una enorme inseguridad jurídica, porque el contenido podía ser borrado o suprimido de buscadores locales (google.es) pero seguía estando en el buscador global (google.com). Postura que contradecía totalmente el protocolo elaborado por el Grupo de Trabajo 29. Y que además desarrollo un procedimiento judicial de la CNIL, organismo responsable de la protección de datos en Francia, frente a Google. Esta postura del buscador, le supuso una sanción de 100.000 euros.

La práctica actual de Google es que el contenido se eliminará de todos los dominios (google.es/.com) siempre y cuando el IP que realiza la búsqueda sea desde Europa. La CNIL rechazó totalmente esta solución porque si se realiza la búsqueda desde cualquier otro lugar del mundo que no sea Europa, seguirá apareciendo la información, de tal forma que se pueden seguir vulnerando nuestros derechos fundamentales.

Google entiende que exigir la retirada universal supondría, entre otras cosas, una interferencia desproporcionada en la libertad de expresión e información. El caso ha llegado al TJUE, cuya respuesta aún no ha sido desvelada.

3. Regulación del derecho al olvido en el RGPD.

En este contexto de inmensas dudas acerca de la definición, el contenido y el alcance del derecho al olvido ve la luz el 25 de Enero de 2012, el Proyecto de Reglamento del Parlamento Europeo y del Consejo para la protección de los ciudadanos en relación con el tratamiento de los datos personales y la libre circulación de dichos datos. Éste es, el hoy conocido y ya mencionado, Reglamento General de Protección de Datos.

Por primera vez se regulaba el derecho al olvido, se codificaba y se le daba alcance. En el ámbito político español el Ministerio de Justicio hizo pública el 27 de Noviembre de 2012 la posición española favorable a una regulación europea del derecho al olvido que buscase el equilibrio idóneo entre la tecnología y las limitaciones existentes en el ámbito de internet. [54]

El derecho al olvido aparece regulado en el artículo 17 del RGPD de la siguiente forma:

1. El interesado tendrá derecho a obtener sin dilaciones indebidas del responsable del tratamiento, la supresión de los datos que le conciernan, el cual estará obligado a suprimir sin dilación indebida, los datos personales cuando concurran alguna de las circunstancias siguientes:
   a) Los datos personales ya no sean necesarios.
   b) El interesado retire el consentimiento.
   c) El interesado se oponga al tratamiento.
   d) Los datos hayan sido tratados ilícitamente.
   e) Los datos deben suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados Miembros.
   f) Los datos personales se hayan establecido en relación con la oferta de servicios de la sociedad de la información mencionada en el articulo 8 (relativas a las condiciones aplicables al consentimiento del niño)

Además en este mismo artículo pero en su apartado tercero se establece cuando no se aplicará el derecho al olvido. Será en las siguientes situaciones:

a) Cuando se esté ejercitando el derecho a la libertad de expresión e información.

[54] "Propuesta de Reglamento sobre Protección de Datos Personales", Ministerio de Justicia, Posición Española/Versión 3.3, 27 Nov 2012, página 18.

b) Cuando sea necesario para el cumplimiento de una obligación legal que requiera el tratamiento de datos, o para el cumplimiento de una misión realizada en interés público.
c) Por razones de interés público en el ámbito de la salud pública.
d) Con fines de archivo de interés público, fines de investigación científica/histórica/estadística en la medida en la que el derecho al olvido pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento.
e) Para la formulación, ejercicio o la defensa de reclamaciones.

Esta es la forma en la que el derecho al olvido es regulado en el Reglamento General de Protección de Datos, pero como se ha comentado, los países tienen potestad para en su regulación nacional desarrollar determinados preceptos. En el Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal, el derecho al olvido aparece en el articulo 15 bajo la rúbrica "derecho de supresión" y el único contenido del precepto es remitir al RGPD. Pero se han presentado algunas enmiendas sobre el asunto, destacando especialmente la Enmienda número 298, propuesta por el Grupo Parlamentario Socialista y cuya idea es añadir un nuevo Titulo a la Ley Orgánica cuyo objetivo es recoger unos derechos digitales y su garantía. Entre esos derechos digitales se encuentra el derecho al olvido, ésta vez sí nombrado como tal. La enmienda 304 es la encargada de recoger ese nuevo contenido sobre el derecho al olvido, quedando de la siguiente forma:

«Artículo 84. Derecho al olvido.
1. Toda persona tiene derecho a que sus datos personales sean cancelados en los servicios de Internet cuando, con el tiempo, puedan devenir inadecuados, no pertinentes o excesivos en relación con los fines para los que se recogieron o trataron y el tiempo transcurrido.
2. Cuando se cumplan los requisitos establecidos en el párrafo anterior, el gestor de un motor de búsqueda estará obligado a eliminar de la lista de resultados, obtenida tras una búsqueda efectuada a partir del nombre de una persona, los vínculos a páginas web publicadas por terceros y que contienen información relativa a esta persona, aunque dicho nombre o información hayan sido lícitamente publicados y no se borren previa o simultáneamente de estas páginas web.

3. Los responsables de redes sociales suprimirán los datos personales facilitados durante su minoría de edad por el afectado o por terceros, a petición del interesado y sin necesidad de invocar justificación adicional alguna.»

En el primer apartado, se resume un concepto del derecho al olvido. En el segundo, la obligación de los buscadores de eliminar el contenido cuando se cumpla lo estipulado en el primer apartado. Y en el tercer y último apartado se garantiza el derecho de los menores de edad a que sus datos sean borrados de las redes sociales.

4. Caso Mario Costeja o Google Spain.

Hace 20 años fueron publicados en un periódico nacional, concretamente La Vanguardia, varios anuncios en los que se mencionaba a Mario Costeja así como su pareja como deudores y se lanzaba la subasta de esas propiedades. Varios años después se procedió a la digitalización de todas las ediciones del mencionado periódico desde 1881, lo que contribuyó en gran medida a que esta información perviviera a través de los años. Ya que con el procedimiento de digitalización, esa información tan vulnerable para Mario fue indexada por Google, lo que quiere decir, que al buscar su nombre en dicho buscador salían directamente enlaces que te llevaban a esos datos.

Así fue como Mario Costeja descubrió en 2009, once años después, que esa información estaba circulando en la red. Una información desfasada, porque en ese transcurso temporal de once años, había pagado sus deudas y estaba divorciado. Fue entonces cuando se dirigió en primer lugar a La Vanguardia pero el periódico se negó a cancelar los datos. En ese momento, se dirigió a la Agencia Española de Protección de Datos para iniciar un procedimiento contra Google, ésta le dio la razón: “Le corresponde a Google adoptar las medidas necesarias para retirar los datos de su índice e imposibilitar el acceso a los mismos". El siguiente paso fue la Audiencia Nacional, la cual tenia bastantes dudas al respecto y lo que hizo fue plantear una cuestión de prejudicial ante el TJUE.

Dos años después, por fin, hubo respuesta.

“Los artículos 12, letra b), y 14, párrafo primero, letra a), de la Directiva 95/46 deben interpretarse en el sentido de que, al analizar los requisitos de aplicación de estas

disposiciones, se tendrá que examinar, en particular, si el interesado tiene derecho a que la información en cuestión relativa a su persona ya no esté, en la situación actual, vinculada a su nombre por una lista de resultados obtenida tras una búsqueda efectuada a partir de su nombre, sin que la apreciación de la existencia de tal derecho presuponga que la inclusión de la información en cuestión en la lista de resultados cause un perjuicio al interesado. Puesto que éste puede, habida cuenta de los derechos que le reconocen los artículos 7 y 8 de la Carta, solicitar que la información de que se trate ya no se ponga a disposición del público en general mediante su inclusión en tal lista de resultados, estos derechos prevalecen, en principio, no sólo sobre el interés económico del gestor del motor de búsqueda, sino también sobre el interés de dicho público en acceder a la mencionada información en una búsqueda que verse sobre el nombre de esa persona. Sin embargo, tal no sería el caso si resultara, por razones concretas, como el papel desempeñado por el interesado en la vida pública, que la injerencia en sus derechos fundamentales está justificada por el interés preponderante de dicho público en tener, a raíz de esta inclusión, acceso a la información de que se trate."[55] **(SENTENCIA TJUE (GRAN SALA) DE 13 DE MAYO DE 2014)**

Fue con esta Sentencia la primera vez que los Tribunales europeos reconocían el derecho al olvido.

Por lo tanto, el derecho al olvido es algo muy novedoso, y que está promoviendo muchos procedimientos pero se están desestimando gran parte de ellos, porque existe una frontera muy delgada entre lo que puede ser considerado como olvido y lo que no. Entra en conflicto con otros derechos, especialmente, el derecho a la libertad de expresión o de información. El TS lo tiene meridianamente claro: "El derecho al olvido no ampara el borrado de una información lícitamente publicada en el pasado la información que se divulgue sea veraz, se refiera a asuntos de interés general o relevancia pública, y no se sobrepase el fin informativo porque se le dé un matiz injurioso, denigrante o desproporcionado."

5. Procedimiento para ejercitar el derecho al olvido y formularios.

[55] Véase, Sentencia Tribunal de Justicia Unión Europea (GRAN SALA) de 13 de Mayo de 2014.

En 2014, tras el reconocimiento del TJUE en el caso Costeja, las solicitudes a Google para llevar a cabo el borrado de datos se dispararon, siendo un total de 171.242.

En la actualidad las solicitudes que le han llegado a Google han sido un total de 662.418, que han supuesto la retirada de más de dos millones de URLs. [56]

La sentencia antes mencionada sentó las bases para llevar a cabo el procedimiento para ejercitar el derecho al olvido.

Ese procedimiento es el siguiente:

1. Solicitar al editor del sitio web en concreto que elimine nuestros datos personales, o al usuario que haya subido la información.
   Por lo tanto, existe la posibilidad de que el usuario pueda hacerlo directamente ante las fuentes de información. Deberá hacerlo mediante un escrito y fotocopia de su documento de identidad.
2. Dirigirse directamente a los buscadores.
   Para poder dirigirte directamente a los buscadores es necesario que no se haya iniciado previamente una reclamación al sitio web concreto.
   Los principales buscadores son Google y Bing, que a través de sus páginas webs, han puesto a disposición de los usuarios sendos formularios para poder solicitar el borrado de datos. Esos formularios son los siguientes:

   Google:[57]

[56] Véase, https://transparencyreport.google.com/eu-privacy/overview?hl=es
[57] Véase, https://www.google.com/webmasters/tools/legal-removal-request?complaint_type=rtbf&visit_id=1-636567859449978620-4109749020&hl=es&rd=1&pli=1

Solicitar la eliminación de contenido indexado en la Búsqueda de Google en virtud de la ley de protección de datos europea

En mayo de 2014, un fallo del Tribunal de Justicia de la Unión Europea (C-131/12, 13 de mayo de 2014) permite que determinados usuarios soliciten que los motores de búsqueda eliminen resultados de consultas que incluyan su nombre si los derechos de privacidad de la persona prevalecen sobre el interés suscitado por dichos resultados.

Al realizar la solicitud, Google buscará un equilibrio entre los derechos de privacidad de los usuarios y el derecho del público a conocer y distribuir información. Al evaluar tu solicitud, Google examinará si los resultados incluyen información obsoleta sobre ti, así como si existe interés público por esa información; por ejemplo, podemos rechazar la eliminación de información sobre estafas financieras, negligencias profesionales, condenas penales o el comportamiento público de funcionarios del Gobierno.

Para completar este formulario, necesitarás una copia digital de un documento de identificación. Si envías la solicitud en nombre de otra persona, tendrás que facilitar un documento de identificación personal de la persona en cuestión.

** Campo obligatorio*

TU INFORMACIÓN

País cuya legislación se aplica a tu solicitud *
Selecciona tu país o tu región

En esta pestaña te solicita tu país para establecer que legislación es aplicable. Solo aparecen paises de la UE, pues solo aquí se puede ejercitar el derecho al olvido.

Nombre legal completo *

Aunque envíes la solicitud en nombre de otra persona que te haya autorizado para representarla, *debes indicar tu nombre*. Si representas a otra persona, debes tener autoridad legal para actuar en su nombre.

Nombre:

Apellidos:

Dirección de correo electrónico de contacto *

Dirección de correo electrónico de contacto *

Actúo en nombre de... *

Si envías esta solicitud en nombre de otra persona, tienes que especificar tu relación con ella (por ejemplo, "padre" o "abogado"). Es posible que te solicitemos documentación que confirme que estás autorizado para representarla.

- Yo mismo
- Cliente
- Familiar
- Amigo
- Otros

Tu relación legal con la persona que ha presentado esta solicitud *

Adjunta una copia legible de un documento que verifique la identidad de la persona que ha presentado la solicitud *

Para evitar las solicitudes de eliminación de contenido fraudulentas de personas que se hacen pasar por otros usuarios, que intentan dañar a sus competidores o que quieren eliminar información legal de forma inadecuada, necesitamos verificar tu identidad. No es necesario que sea un pasaporte ni otro documento de identificación oficial. Puedes ocultar partes del documento (por ejemplo, el número de identificación), siempre que el resto de la información permita identificarte. Asimismo, puedes ocultar la fotografía, excepto si solicitas que se eliminen páginas que incluyan fotografías tuyas. Google solo utilizará esta información para certificar la autenticidad de tu solicitud y eliminará la copia en un plazo de un mes una vez que se haya cerrado la solicitud de eliminación de contenido (a menos que la ley establezca lo contrario).

Para subir varios documentos a la vez, mantén pulsada la tecla Ctrl o Comando al seleccionar los archivos.

Elegir archivos Ningún archivo seleccionado

¿Has presentado una solicitud anterior?

Si ya has solicitado que retiremos URLs con contenido similar, podremos ayudarte antes si, en vez de enviarnos un nuevo mensaje, contestas al correo electrónico que te hemos enviado.

Si prefieres enviarnos un mensaje nuevo, introduce el número de referencia de 14 dígitos que identifica tu solicitud anterior. El formato sería 1-1111000001111, por ejemplo. Lo encontrarás en el asunto del correo electrónico que te hemos enviado.

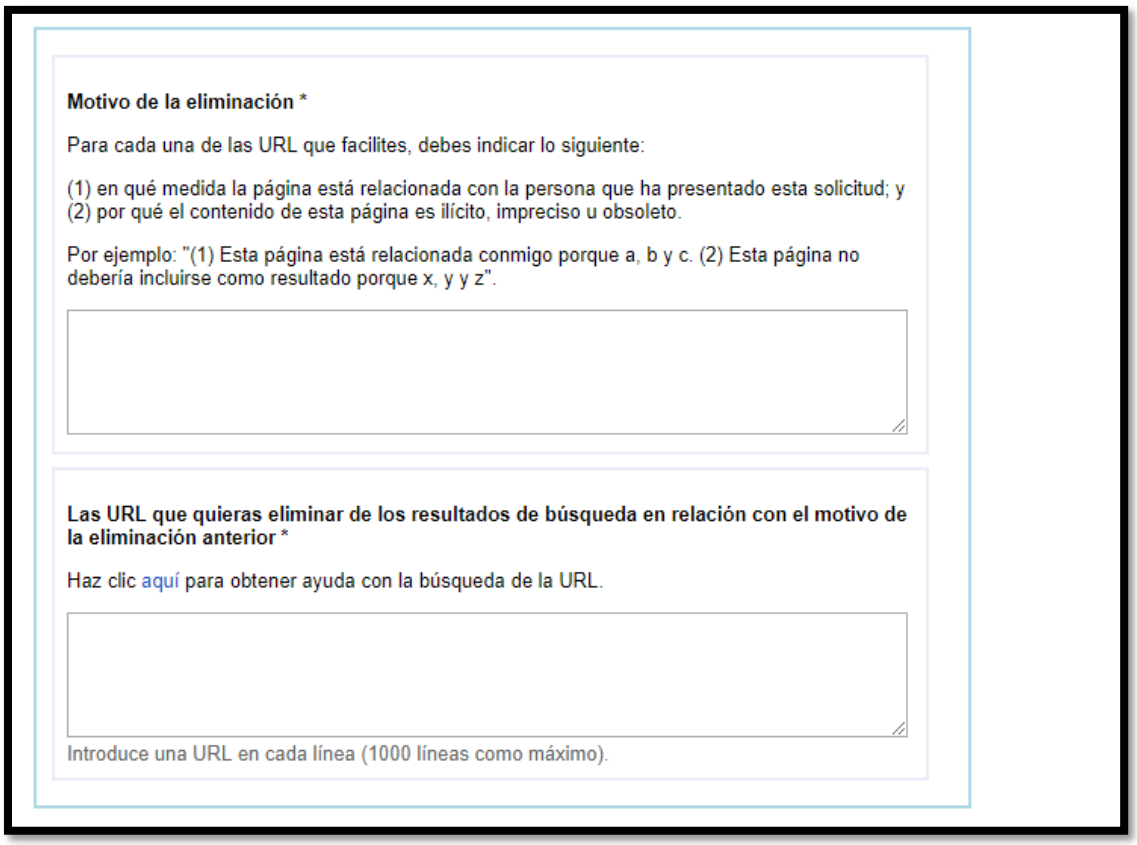
IDENTIFICAR LOS RESULTADOS DE BÚSQUEDA QUE QUIERAS QUE SE ELIMINEN

Nombre utilizado para realizar búsquedas *

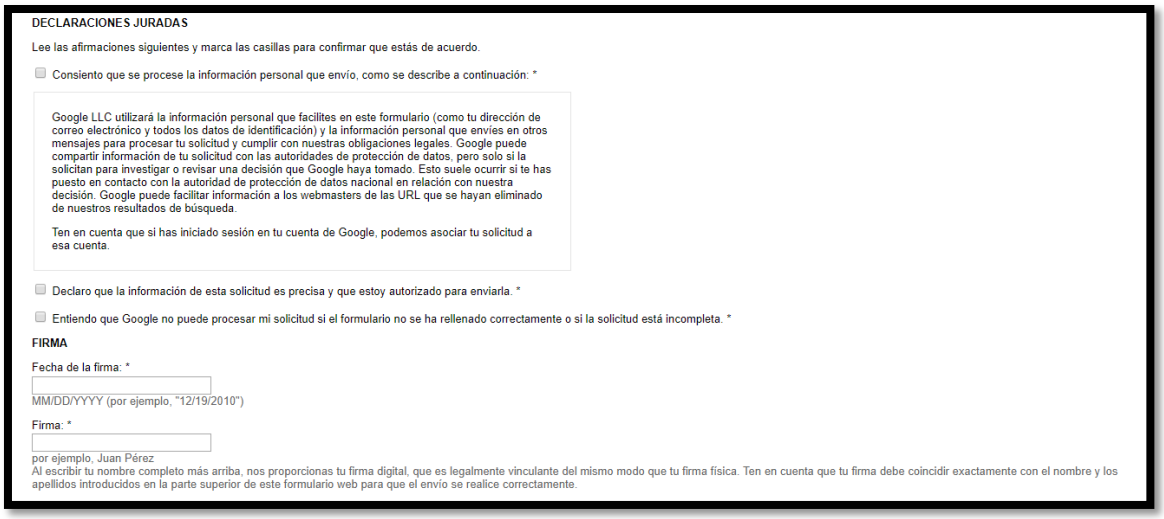
Este debería ser el nombre que, si se utiliza como consulta de búsqueda, produzca los resultados que quieres eliminar del registro. Si quieres enviar varios nombres (por ejemplo, si tu apellido de soltera es diferente al que utilizas ahora), utiliza una barra diagonal ("/") para separarlos. Por ejemplo, "Ana García / Ana Díaz".

Si esta notificación está relacionada con varios motivos que han sido objeto de una infracción, envía únicamente el primero aquí abajo. A continuación, haz clic en el enlace "Añadir un nuevo grupo" que aparece debajo de los cuadros de texto para añadir otro motivo.

En este apartado te pide que añadas el nombre que has usado para la búsqueda que ha generado el contenido que quieras eliminar. Te permite poner varios nombres, por ejemplo si has cambiado de apellido.



Por cada enlace que se añada, se debe incorporar en qué grado esa información está relacionada con la persona agraviada y el motivo por el cual el contenido de ese enlace es ilícito, impreciso u obsoleto.



DECLARACIONES JURADAS

Lee las afirmaciones siguientes y marca las casillas para confirmar que estás de acuerdo.

Consiento que se procese la información personal que envío, como se describe a continuación: *

Google LLC utilizará la información personal que facilites en este formulario (como tu dirección de correo electrónico y todos los datos de identificación) y la información personal que envíes en otros mensajes para procesar tu solicitud y cumplir con nuestras obligaciones legales. Google puede compartir información de tu solicitud con las autoridades de protección de datos, pero solo si la solicitan para investigar o revisar una decisión que Google haya tomado. Esto suele ocurrir si te has puesto en contacto con la autoridad de protección de datos nacional en relación con nuestra decisión. Google puede facilitar información a los webmasters de las URL que se hayan eliminado de nuestros resultados de búsqueda.

Ten en cuenta que si has iniciado sesión en tu cuenta de Google, podemos asociar tu solicitud a esa cuenta.

Declaro que la información de esta solicitud es precisa y que estoy autorizado para enviarla. *

Entiendo que Google no puede procesar mi solicitud si el formulario no se ha rellenado correctamente o si la solicitud está incompleta. *

FIRMA

Fecha de la firma: *

MM/DD/YYYY (por ejemplo, "12/19/2010")

Firma: *

por ejemplo, Juan Pérez

Al escribir tu nombre completo más arriba, nos proporcionas tu firma digital, que es legalmente vinculante del mismo modo que tu firma física. Ten en cuenta que tu firma debe coincidir exactamente con el nombre y los apellidos introducidos en la parte superior de este formulario web para que el envío se realice correctamente.

Por último se procede a aceptar las condiciones, así como a firmar dicha solicitud.

3. Si el buscador no respondiese o se considere que la respuesta recibida no es la adecuada, puede solicitar a la Agencia Española de Protección de Datos que tutele su derecho.[58]

   Para que la Agencia Española de Protección de Datos pueda tramitar su reclamación en caso de no haber sido atendida su solicitud de ejercicio del derecho de supresión, resulta necesario que el responsable no haya hecho efectivo el derecho, y aporte alguno de los siguientes documentos:

- la negativa del responsable del tratamiento a la supresión de los datos solicitados.
- copia sellada por el responsable del tratamiento del modelo de petición de supresión.
- copia del modelo de solicitud de acceso sellada por la oficina de correos o copia del resguardo del envío por correo certificado.
- cualesquiera otros medios de prueba facilitados por el responsable del tratamiento y de los que se pueda deducir la recepción de la solicitud.

[58] Véase, https://www.aepd.es/media/formularios/formulario-derecho-de-supresion.pdf

CONCLUSIONES

El siglo XXI es el siglo de la tecnología. Los avances tecnológicos inundan nuestras vidas, y en ocasiones, incluso, se apoderan de ella. Su protagonismo en el día a día de nuestra sociedad es de tal envergadura, que por un lado nos facilita nuestra existencia pero por otro, puede poner (y pone) en jaque nuestros derechos y libertades más fundamentales.

Es por ello que si el siglo XXI es el siglo de la tecnología; el derecho a la protección de datos debe ser el derecho de este siglo. Porque es el mecanismo perfecto para protegernos ante las injerencias que podemos sufrir por el elevado consumo de nuevas tecnologías.

De tal forma, que partiendo de la base de la importancia del derecho a la protección de datos, era necesaria una nueva regulación. No se puede combatir al siglo de oro de la tecnología con legislaciones del siglo pasado, que no ofrecen el ámbito de protección suficiente. Por lo tanto, el Reglamento General de Protección de Datos llegó cuando tenía que llegar. En 2015. En el estallido de la informática. Justo en el momento en el que las redes sociales han consagrado un nuevo estilo de vida. En el mismo año en el que la RAE incorpora a su diccionario palabras como “tuit”, “hacker” o “pantallazo”. Siendo 2015 también el primer año en el que Facebook es denunciado por vulnerar la privacidad de sus usuarios, e incluso, se comienza a investigar una posible transferencia de datos de Facebook a Estados Unidos. Fue el año en el que construyó drones para llevar Internet a aldeas remotas, y Google terminó su proyecto de globos aerostáticos para llevar Internet a Indonesia. Por lo tanto, sí, 2015 era el año.

En este contexto, “nació” el RGPD. Con diversos objetivos, pero el principal, armonizar las legislaciones existentes en torno a esta materia. Porque que, cada país de la Unión Europea tuviese una legislación sobre Protección de Datos, solo creaba inseguridad jurídica. Este Reglamento quería romper en muchos sentidos con la legislación que habíamos tenido hasta el momento, desarrollándose una normativa de marcado carácter anglosajón. Y de este carácter se derivan, probablemente, los que son los dos pilares fundamentales del Reglamento: la responsabilidad proactiva y las medidas sancionadoras.

La responsabilidad proactiva lo que hace es poner sobre la mesa un concepto muy claro, "prevención". Hay que adelantarse a los riesgos, preveerlos. Anticiparse. Y las medidas sancionadoras, quieren infringir temor. Hablamos de multas de hasta veinte millones de euros o el 4% del valor de la empresa.

Pero el Reglamento no es un salvador. Han pasado tres años desde que fue creado hasta su entrada en vigencia. Tres años en los que se han desarrollado nuevos delitos relacionados con los datos y la informática, en los que se han confirmado el "escape" de datos de usuarios de Facebook a empresas privadas y un largo etcétera. Es probable, que en algunos aspectos, el Reglamento nazca ya anticuado.

Además, ha introducido tantas novedades, que en la teoría resultan buenas ideas pero que no se sabe cómo se van a desarrollar en la práctica. Un ejemplo de ello es el derecho al olvido, regulado por primera vez en esta nueva norma. Google ya ha dejado clara su postura de que el derecho al olvido es cosa de Europa. Por lo tanto, los datos serán borrados dentro de este continente, pero podrás seguir accediendo a ellos desde IP que estén en otro lugar del mundo. Eso no es una protección suficiente, eso no es un derecho al olvido, por lo que probablemente sea cierto aquello de que Internet no olvida. Como ya dijera en 2010 Viviane Reding: "Dios perdona y olvida; pero Internet nunca lo hace."

Y no solo eso, el Reglamento General de Protección de Datos, también supondrá un quebradero de cabeza para las empresas. Para todas. Empezando por esa necesidad de modificar la forma de pedir el consentimiento, sea online u offline. Y acabando por esa figura novedosa, como es el Delegado de Protección de Datos, que será obligatoria en muchas entidades. El principal problema de todo esto, es que las empresas no saben cómo hacer frente a las numerosas novedades que ha provisto el Reglamento. Esto se refleja en que un tanto por ciento mínimos ya está cumpliendo con el Reglamento.

En definitiva, el Reglamento General de Protección de Datos era necesario. Se necesitaban regular nuevos derechos y garantías, así como incrementar las sanciones. Las empresas deben saber que los datos no son algo nimio. La protección debe estar al mismo nivel que el uso que hacemos de las nuevas tecnologías. Además, en el ámbito nacional, también tenemos que esperar a ver el resultado final del Anteproyecto. Mientras tanto, tendremos que observar cómo se desarrolla en la práctica la nueva legislación europea y si es capaz de hacer frente a los grandes gigantes de nuestra época.

BIBLIOGRAFÍA

LIBROS/ARTICULOS DE REVISTAS

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, *Guía del Reglamento General de Protección de Datos para responsable del tratamiento,* 2017

FLAHERTY, D.H. *Privacy in Colonial New England,* 1972.

GALAN MUÑOZ, A. *La protección jurídica de la intimidad y de los datos de carácter personal frente a las nuevas tecnologías de la información y comunicación.* Ed. Tirant lo Blanch, Valencia, 2011

GARCIA GUERRERO, JL. *Los derechos fundamentales a la vida, la igualdad, y los derechos de libertad.* Ed. Tirant lo Blanch, Valencia, 2013.

GUERRERO PICO, M.C. *El impacto de Internet en el Derecho Fundamental a la protección de datos de carácter personal.* Ed. Civitas, Pamplona, 2006.

HEREDERO HIGUERAS, M. *La sentencia del Tribunal Constitucional de la Republica Federal Alemana relativa al censo de población de 1983.* Documento administrativo, número 198.

MARTINEZ R. *El derecho fundamental a la protección de datos: perspectivas.* Revista de Internet, Derecho y Político. 2007.

MURILLO DE LA CUEVA, P.L. *Perspectivas del derecho a la autodeterminación informativa,* Revista de Internet, Derecho y Política. 2007

PEREZ ROYO, J. *Curso de Derecho Constitucional.* Ed. Marcial Pons, Madrid, 2016.

RALLO LOMBARTE, A. *El derecho al olvido, Google versus España.* Ed. Centros de Estudios Políticos y Constitucionales.

SALDAÑA, M.N. "*The right to privacy", La génesis de la privacidad en el sistema constitucional norteamericano: El centenario legado de Warren y Branderis.* Revista de Derecho Politico, número 85. Septiembre – Diciembre 2012.

WARREN, S.D y BRANDEIS L.D. *El derecho a la intimidad,* 1995.

LEGISLACIÓN

Declaración Universal de Derechos Humanos.

Convenio Europeo para la protección de los derechos humanos y libertades fundamentales del Consejo de Europa.

Convenio Nº 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.

REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). (RGPD)

Constitución Española de 1978.

Ley Orgánica 5/1992, de 29 de Octubre, de Regulación del Tratamiento Automatizado de Datos de carácter personal. Derogada por la LOPD. (LORTAD)

Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal.

SENTENCIAS

Sentencia Tribunal Justicia Europea (Gran Sala) de 13 de Mayo de 2014.

Sentencia Tribunal Constitucional 94/1998, de 4 de Mayo de 1998.

Sentencia Tribunal Constitucional 254/1993, de 20 de Julio de 1993.

Sentencia Tribunal Constitucional 292/2000, de 30 de Noviembre de 2000.

Sentencia Tribunal Constitucional 39/2016, de 3 de Marzo de 2016.

Sentencia Audiencia Nacional de 29 Diciembre de 2014, número de recurso 725/2010.

PÁGINAS WEBS

http://www.agpd.es/portalwebAGPD/CanalDelCiudadano/derechos/principales_derchos/acceso-ides-idphp.php

http://www.agpd.es/portalwebAGPD/CanalDelCiudadano/derechos/principales_derchos/rectificacion-ides-idphp.php

http://www.agpd.es/portalwebAGPD/CanalDelCiudadano/derechos/principales_derchos/cancelacion-ides-idphp.php
http://www.agpd.es/portalwebAGPD/CanalDelCiudadano/derechos/principales_derchos/oposiciop-ides-idphp.php
http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/infografias/Adaptacion_RGPD_sector_privado.pdf.
http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/GuiaG/2018/AnalisisDeRiesgosRGPD.pdf

http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/GuiaG/2018/Guia_EvaluacionesImpacto.pdf

http://www.agpd.es/portalwebAGPD/canaldocumentacion/docu_grupo_trabajo/wp29/cocomm/Traduc_oficial_ult_version/wp243revol_es.pdf
http://transparencyreport.google.com/eu-privacy/overview?hl=es
https://www.google.com/webmasters/tools/legal-removal-request?complaint_type=rtbf&visit_id=1-636567859449978620-4109749020&hl=es&rd=1&pli=1

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

http://sedeagpd.gob.es/sede-electronica-web/vistas/formReclamacionDerechos/previoReclamacionDerecho.jsf

OTROS DOCUMENTOS

V Informe 2016 de Infoempleo – Adeco sobre redes sociales y mercado de trabajo.

Building Trust in Europe's Online Single Market. Speech at the American Chamber of Commerce to the EU. Brussels, 22 June 2010

Propuesta de Reglamento sobre Protección de Datos, Ministerio de Justicia. Posición española. Versión 3.3