Universidad de Alcalá

LA EVOLUCIÓN NORMATIVA DEL DERECHO A LA PROTECCIÓN DE DATOS

"El Nuevo Reglamento Europeo 2016/679"

THE NORMATIVE EVOLUTION OF THE RIGHT TO DATA PROTECTION

"The New European Regulation 2016/679"

Máster Universitario en

Acceso a la Profesión de Abogado

Presentado por:

Dª MONIKA KATARZYNA GOLINSKA

Codirigido por:

Dr. MIGUEL MARCOS AYJÓN

Y Dr. ESTEBAN MESTRE DELGADO

Alcalá de Henares, a 19 de febrero de 2018.

ÍNDICE

RESUMEN..... 4

I. INTRODUCCIÓN..... 5

II. EVOLUCIÓN NORMATIVA DEL DERECHO A LA PROTECCIÓN DE DATOS

1.La protección de datos como derecho fundamental en la Constitución Española 8

2.La evolución del derecho europeo 13

2.a La Carta de los Derechos Fundamentales..... 15

2.b Jurisprudencia del TEDH 17

2.c Art. 16 TFUE..... 19

III. EL NUEVO REGLAMENTO EUROPEO

1. EL Reglamento General de Protección de Datos de 27 de abril de 2016..... 20

2. El por qué de la nueva regulación europea..... 23

3. El objeto del RGPD..... 25

4. Estructura del RGPD..... 26

5. Ámbito de aplicación material 27

6. Concepto y definiciones básicas 28

7. Principios de protección de datos en la nueva normativa…….....29

8. Tratamiento de categorías especiales de datos…….....38

9. Los derechos del interesado y las obligaciones del responsable……..…40

9.1 Las obligaciones del responsable…….....41

9.2 Los derechos del interesado 43

10. El responsable o corresponsable de tratamiento y sus responsabilidades 49

11. Control del cumplimiento mediante sanciones y multas..... 54

IV. Conclusiones..... 55

V. Bibliografía 58

VI. Sentencias y recursos web……...……58

RESUMEN

La creciente evolución tecnológica en continuo desarrollo supone una evolución normativa y el surgimiento de derechos nuevos que han de ir regulándose e incorporándose a las normativas por parte del legislador. El derecho está en continuo desarrollo persiguiendo la realidad social y ajustando conceptos o realidades a través de las normas.

Con el desarrollo de internet, que podríamos llamar la revolución industrial del BIG DATA, desde luego los derechos que más se vieron perjudicados son los contenidos en el art. 18 de la CE. La privacidad, el honor, la intimidad y la vida familiar se ven comprometidos cada vez más y ello requiere de una regulación estricta en este sentido. Regulación que seguramente vaya a avanzar con el avance de la inteligencia artificial desarrollada en estos momentos por grandes empresas mundiales.

Hasta la aparición de la normativa europea y concretamente hasta el desarrollo del Convenio 108 del Consejo de Europa no se había definido en España el alcance del derecho a la protección de datos[1]. Dicho Convenio, en palabras de JULIAN VALERO TORRIJOS inspiró al Tribunal Constitucional en la elaboración y confirmación del derecho a la protección de datos y a su formación como un derecho fundamental, autónomo e independiente.

Este trabajo pretende mostrar el camino que ha recorrido la formación de dicho derecho fundamental a la protección de datos, teniendo en cuenta la normativa europea y la normativa española, así como algunas normativas europeas adoptadas a raíz del nuevo Reglamento de Protección de Datos (UE) 2016/679 de 27 de abril de 2016 (en adelante RGPD), haciendo especial hincapié en las novedades introducidas por el mismo.

PALABRAS CLAVE:

Big Data. Derechos fundamentales. Evolución tecnológica. Legislación europea. Regulación de protección de datos.

ABSTRACT

The growing technological evolution in continuous development implies a normative evolution and the emergence of new rights that must be regulated and incorporated into the regulations by the legislator. The law is in continuous development pursuing the social reality and adjusting concepts or realities through the rules.

With the development of the internet, which we could call the industrial revolution of BIG DATA, of course the rights that were most affected are those contained in art. 18 of the EC. Privacy, honor, privacy and family life are increasingly compromised and this requires strict regulation in this regard. Regulation that will surely advance with the advance of artificial intelligence developed at this time by large global companies.

Until the emergence of European legislation and specifically until the development of Convention 108 of the Council of Europe had not been defined in Spain the scope of the right to data protection. This Agreement, in the words of JULIAN VALERO TORRIJOS, inspired the Constitutional Court in the elaboration and confirmation of the right to data protection and its formation as a fundamental, autonomous and independent right.

This work aims to show the path that has taken the formation of this fundamental right to data protection, taking into account European regulations and Spanish regulations, as well as some European regulations adopted as a result of the new Data Protection Regulation (EU) 2016/679 of April 27, 2016 (hereinafter RGPD), with special emphasis on the novelties introduced by it.

KEYWORDS:

Big Data. Fundamental rights. Technological evolution. European legislation. Data protection regulation.

I.INTRODUCCIÓN

"Compartir es bueno, y con la tecnología digital, compartir es sencillo". Las palabras de Richard Stallman, el famoso hacker del Laboratorio de Inteligencia Artificial del Instituto Tecnológico de Massachusetts (MIT), adquieren, con el paso del tiempo, un significado que seguramente ni su propio autor se imaginaba. De hecho, compartir a día de hoy es tan sencillo que resulta hasta difícil de controlar. Cualquier cosa que compartamos puede tener el efecto boom inmediato y expandirse por todo el mundo en cuestión de horas.

Ya en 1971 aquel famoso estudiante de la Universidad de Harvard tomaba conciencia en cuanto a la comunicación de la información y en cuanto a la sencillez de manejo de la misma. Gracias a grandes avances tecnológicos el ser humano ha convertido el mundo virtual en una gran base de datos de información a la que cualquier persona, en mayor o menor medida puede acceder. Ello ciertamente supone que estemos informados y podamos expandir nuestros conocimientos, pero por otro lado y en palabras de Alan Moore, el famoso guionista y escritor, "la tecnología es siempre un arma de doble filo, traerá muchos beneficios, pero también muchos desastres" y por ello hay que establecer límites.

A medida que avanza la tecnología cambia la realidad y la percepción de las mismas cosas. La investigación y el manejo de la información acarrean beneficios para una parte de la población y perjuicios para la otra. El manejo de las grandes bases de datos proporcionados por los usuarios de ciberespacio supone la intromisión en la vida de la población. Los datos de diversa índole (datos sobre nuestros gustos, sobre las preferencias, sobre las cosas que poseemos, sitios que frecuentamos, datos sobre la salud), que actualmente no se recogen en papel, sino en ficheros automatizados, son objeto de fácil transmisión y manipulación.

Incluso desde los principios del cine el ser humano fue imaginando la evolución y el predominio de las máquinas, así como, la capacidad de estas de procesar la información. Precisamente a partir de ello deriva el poder, ya que la misma proporciona soluciones o estrategias lógicas deducibles, que en una mente perversa pueden provocar

los deseos un tanto alejados de la ética y del bienestar de la sociedad, llegando incluso a manipulación maliciosa de la misma.

Los gigantes de la industria de internet, como Google, Facebook, Apple o Microsoft, pioneros en el manejo de las "big data", fortalecen cada vez más sus posiciones debido a la continua rivalidad política entre todos los países del mundo. Los usuarios de las redes sociales, páginas web, y los servicios de compra venta a través de sistemas e-commerce, proporcionan gran cantidad de huellas referentes a su vida personal y que, posteriormente, dichas compañías guardan con fines diversos, utilizando normalmente la excusa de mejorar el servicio para el futuro del usuario. De este modo, inconscientemente dejamos que se nos proporcione publicidad o ciertos elementos escogidos de acuerdo con nuestras aficiones o preferencias, de modo que, aunque el usuario no se dé cuenta, obedece a cierta "manipulación" por parte de las empresas. La publicidad encamina al consumidor a comprar, y por ello en la vida real (no virtual) está sometida a control por parte de los estados a través de las normativas. Sin embargo, este control no alcanzaba el ciberespacio. Además, la libre disposición sobre ciertos aspectos de la vida de un individuo puede constituir una intromisión en su vida privada, suponer aprovecharla a cambio de un precio o a cambio de otra cosa y sobre todo someterlo a un control muy estricto de su vida, dando lugar sobre todo a la ciberdelincuencia.

El control más estricto y quizá el más temido por ser humano se lleva a cabo por parte del Estado. El ejercicio del poder por parte de este se encuentra sometido al imperio de la Ley. Ahora bien, con los progresos tecnológicos ha evolucionado también la administración de los gobernados. Tengamos en cuenta que hasta poco nos veíamos obligados a recopilar gran cantidad de datos manualmente y que actualmente se recogen en ficheros automatizados, plataformas y programas específicos que son capaces de cruzar datos sobre un individuo en concreto y someterlo a un control estricto por parte del sistema. La creación de la Administración electrónica facilita la comunicación entre la misma y las personas, pero por otro lado constituye una herramienta de vigilancia con un margen de error muy poco probable. Pongamos como ejemplo la Agencia tributaria, con sistemas de cruce de datos a la hora de comprobar la veracidad de los datos proporcionados en cuanto a la declaración de la renta. Otro ejemplo es el DNI electrónico, los controles establecidos en cuanto al pago con dinero en efectivo, el sistema cl@ve, etc. La realidad es que dentro de poco lo más probable que todos los

pagos se realicen a través de tarjetas y que gran parte la comunicación con el Estado se convertirá en un control automático en el que el consentimiento del administrado no tendrá una relevancia prioritaria.

Por todo ello existe una gran preocupación por parte de los Estados en cuanto a la libre disposición de la información, comunicación y datos personales. En el seno europeo empiezan a mostrarse serias iniciativas en cuanto a la protección de la vida privada de las personas físicas respecto a los bancos de datos electrónicos en el sector privado mediante la Resolución nº 73, de 26 de septiembre de 1973, del Comité de Ministros del Consejo de Europa, y posteriormente la relativa a la protección de las personas físicas pero referente al sector público, mediante la Resolución nº 74, de 20 de septiembre de 1974. Asimismo, en Estados Unidos en el mismo año surge el Privacy Act a raíz de la creación del sistema ARPANET en el año 1969[2], que fue diseñado por el sistema de defensa de los Estados Unidos y que muestra el primer intercambio de datos de un ordenador a otro a través de una línea telefónica. Posteriormente surgen INTERNET y el WWW. A partir de esta revolución de intercambio global de datos brota precisamente una seria necesidad internacional de proteger los derechos de las personas. En la actualidad tiene más de 2.300 millones de usuarios y un tráfico de alrededor de 27 mil *petabytes* (PB) por mes[3].

El desarrollo constante de la tecnología supone pues un desarrollo constante de la Ley que protege la esfera individual de las personas y somete a su vez los imperios y las potestades de entes o Estados a un control en lo que a la telemática se refiere. El objeto de presente trabajo es estudiar el desarrollo normativo en la materia de protección de datos a nivel nacional y europeo, analizando los principios que rigen en la misma, los procedimientos para la protección del derecho y las posibles amenazas relacionadas con el constante desarrollo tecnológico.

[2] TRIGO ARANDA, VICENTE, *"Historia y evolución de internet"*, Revista Digital Autores Científico-Técnicos y Académicos;pág.2; Martes, 25 Diciembre 2012 11:05

[3] http://www.evolutionoftheweb.com/, http://www.evolutionoftheweb.com/?hl=es#/growth/day , Consultado 16.02.2018, 20:42

II. EVOLUCIÓN NORMATIVA DEL DERECHO A LA PROTECCIÓN DE DATOS

1.La protección de datos como derecho fundamental en la Constitución Española.

La Constitución española en su art.18.4 recoge una limitación al uso de la informática para **"**garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos". Introduce de esta manera por un lado una limitación para quienes hagan uso de las herramientas informáticas y, por otro, recoge una tutela de derechos relacionados con el honor, la intimidad personal y familiar, garantizando asimismo el pleno ejercicio de sus derechos. Posiblemente el inciso más importante es la limitación de la informática y la garantía del pleno ejercicio de los derechos, ya que se puede intuir la protección del individuo, no en relación al derecho a la intimidad o al derecho al honor, sino como un derecho autónomo e independiente de los mismos. Pero tuvo que ser sin embargo un análisis largo y exhaustivo de los tribunales el que llevase concluyendo y reconociendo la protección de datos como un "derecho fundamental" y posteriormente reconociéndolo como autónomo e independiente".

Tal vez el primer pronunciamiento en este sentido lo hizo la Sentencia 94/1998, del Tribunal Constitucional[4], que configura por primera vez el derecho a la protección de datos como un **derecho fundamental**, que engloba la facultad de la persona de controlar sus datos, su uso y su destino. De modo que el ciudadano puede oponerse a que determinados datos personales sean usados para fines distintos a aquél que justificó su obtención. Asimismo, en la STC 96/2012, en su FJ 6, subraya el TC que la protección de datos deriva del art.18.4 CE. Sin embargo, es realmente a partir de la

[4] FJ. 6: *"En suma, ha de concluirse que tuvo lugar una lesión del art. 28.1 en conexión con el art. 18.4 C.E. Este no sólo entraña un específico instrumento de protección de los derechos del ciudadano frente al uso torticero de la tecnología informática,* ***sino que consagra un derecho fundamental autónomo a controlar el flujo de informaciones que conciernen a cada persona*** *-a la «privacidad» según el neologismo que reza en la Exposición de Motivos de la L.O.R.T.A.D., pertenezcan o no al ámbito más estricto de la intimidad, para así preservar el pleno ejercicio de sus derechos. Trata de evitar que la informatización de los datos personales propicie comportamientos discriminatorios"*

Sentencia 292/2000, del Tribunal Constitucional, de 30 de noviembre[5] (recurso de inconstitucionalidad 1463-200, promovido por el Defensor del Pueblo), respecto de los artículos 21.1 y 24.1 y 2 de la LOPD, donde se considera el derecho a la protección de datos como un derecho **autónomo e independiente, "***que a diferencia del derecho a la intimidad del art. 18.1, con quien comparte el objetivo de ofrecer una protección constitucional eficaz de la vida privada 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 art. 18.4 CE debe limitar el uso de la informática, bien desarrollando el derecho fundamental a la protección de datos (art.81.1CE), bien regulando su ejercicio (art.53.1CE). La peculiaridad de este derecho fundamental a la protección de datos respecto de aquel derecho fundamental a 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*****"** (FJ5). El TC aplica esta doctrina teniendo en cuenta los debates previos a la aprobación del texto constitucional, que tuvieron lugar en el año 1977. La discusión sobre la inclusión o no del apartado cuarto del art. 18 de la Constitución suscitó un debate en el cual distintos partidos políticos expresaron sus opiniones. De entre tantos algunos fueron partidarios de no incluir dicho apartado considerando que quedaba protegido por el derecho a la intimidad consagrado en el apartado primero del artículo 18, pero otros tantos consideraron que se trata de un uso de la informática que, aunque por aquel entonces tuvo un desarrollo menor, ha de ser regulado de manera independiente puesto que abarca una gran cantidad

[5] FJ,5: *"Pues bien, en estas decisiones el Tribunal ya ha declarado que el art. 18.4 CE contiene, en los términos de la STC 254/1993, un instituto de garantía de los derechos a la intimidad y al honor y del pleno disfrute de los restantes derechos de los ciudadanos que,* ***además, es en sí mismo "un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos, lo que la Constitución llama 'la informática'", lo que se ha dado en llamar "libertad informática"*** *(FJ 6, reiterado luego en las SSTC 143/1994, FJ 7, 11/1998, FJ 4, 94/1998, FJ 6, 202/1999, FJ 2). La garantía de la vida privada de la persona y de su reputación poseen hoy una dimensión positiva que excede el ámbito propio del derecho fundamental a la intimidad (art. 18.1 CE), y* ***que se traduce en un derecho de control sobre los datos relativos a la propia persona. La llamada "libertad informática" es así derecho a controlar el uso de los mismos datos insertos en un programa informático (habeas data) y comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención*** *(SSTC 11/1998, FJ 5, 94/1998, FJ 4)".*

de datos que pudieran implicar la vulneración de otros preceptos constitucionales más importantes[6].

Según la mencionada Sentencia, el objeto del derecho a la protección de datos alcanza "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 CE 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"**.

En palabras de PARDO LOPEZ, "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 las potenciales agresiones a la dignidad y a la libertad de la persona, provenientes de uso ilegítimo del tratamiento mecanizado de datos, que la Constitución ha venido a llamar "la informática""[7].

Sin embargo, este derecho, al igual que los restantes, está sujeto a límites establecidos legalmente y que se ponen de relieve con la **Sentencia 39/2016, de 3 de marzo (Pleno).** La misma establece como límite al derecho fundamental a la protección

---

6 HERNÁNDEZ-LÓPEZ, J.M. *"El Derecho a la Protección de Datos Personales en la Doctrina del Tribunal Constitucional"*., Nº31, páginas 47-52. Cuadernos Thomson Reuters, Aranzadi,2013 *"Creemos que el tema de la informática es fundamental, aunque hoy sólo se encuentre en los inicios. Por eso, debemos dar una referencia explícita que no sólo atienda a la defensa del honor, de la intimidad personal, que son fundamentales, sino también al pleno ejercicio de los derechos y libertades reconocidos en la Constitución. Se trata de establecer garantías de control de los controladores".*

[7] PARDO LÓPEZ MARÍA.M., "La Protección de Datos Personales en Internet ante la Innovación Tecnológica" Coordinador VALERO TORRIJOS J.,pág.103., ed. Thomson Reuters Aranzadi,2013

de datos **el juicio de la proporcionalidad entre la facultad de control del empresario y el derecho a la protección de datos del trabajador,** de modo que el límite legal consiste en el marco de la relación laboral de la que se deriva la facultad del empresario de dirigir y controlar a sus trabajadores con el fin de que cumplan sus obligaciones contractuales, para lo cual no necesita el consentimiento del trabajador para recoger sus imágenes en el lugar de trabajo, pero sí se requiere que **previamente el mismo esté informado** de la instalación de las cámaras de videovigilancia, información que consiste en este caso en una pegatina que avisa sobre la existencia de las cámaras de videovigilancia, por tanto no es una información expresa[8]. Esta sentencia fue puesta en entredicho por un voto particular[9], el cual recalca la prevalencia de los derechos de

[8] FJ,3: *"La dispensa del consentimiento se refiere, así, a los datos necesarios para el mantenimiento y cumplimiento de la relación laboral, lo que abarca, sin duda, las obligaciones derivadas del contrato de trabajo. Por ello un tratamiento de datos dirigido al control de la relación laboral debe entenderse amparado por la excepción citada, pues está dirigido al cumplimiento de la misma. Por el contrario, el consentimiento de los trabajadores afectados sí será necesario cuando el tratamiento de datos se utilice con finalidad ajena al cumplimiento del contrato*."

[9] *"Tales argumentaciones se sostienen con naturalidad y desenvoltura, pese a haberse recordado en la primera parte de la Sentencia que el deber de información previa forma parte del contenido esencial del derecho a la protección de datos (art. 18.4 CE [RCL 1978, 2836]), actuando como un complemento indispensable de la necesidad de consentimiento del afectado. En un contexto argumentativo como el expuesto, hay base para inferir que un acto de control empresarial encuadrable por su finalidad en el art. 20.3 LET, pero ejercido antijurídicamente y contra lo previsto en el art. 5 LOPD (RCL 1999, 3058) , puede prevalecer sobre el derecho fundamental del art. 18.4 CE (RCL 1978, 2836) y sobre la doctrina de este Tribunal, sentada en las SSTC 292/2000, de 30 de noviembre (RTC 2000, 292) , y 29/2013, de 11 de febrero (RTC 2013, 29) , si así se dedujera tras el pertinente juicio de ponderación y proporcionalidad efectuado. Si mi apreciación no quedara desmentida, una tesis semejante constituiría, sencillamente, un despropósito jurídico-constitucional, pudiendo arrastrar un caudal de consecuencias prácticas de imposible aceptación en nuestro Estado social". "Acaso, el tránsito por camino tan espinoso puede haber sido debido a la desatención hacia la STC 29/2013, de 11 de febrero (RTC 2013, 29) , que expresamente recordaba* ***que la Constitución ha querido que la ley, y sólo la ley, pueda fijar los límites a un derecho fundamental.*** *Pero sea como fuere y más allá de la razón determinante, me resulta imposible admitir que el derecho de los trabajadores a ser informados sobre la suerte de los datos obtenidos por su empleador,* ***derecho este que forma parte del núcleo fuerte del habeas data,*** *pueda concretarse en una mera pegatina con el correspondiente distintivo visible en un cristal, una vez cumplido, eso sí, en contenido y diseño – como recuerda la Ponencia aprobada - el sin duda trascendente Anexo de la Instrucción citada. Contrariando de manera frontal la doctrina sentada por este Tribunal, según la cual el afectado o los afectados por la captación han de conocer el contenido de las imágenes captadas y el propósito perseguido por la implantación de sistemas de video- vigilancia, ahora se sostiene que, una vez insertado el distintivo y cumplidos los Anexos, ya no es preciso especificar* ***"la finalidad exacta que se le ha asignado a ese control", pues lo único importante será determinar si "el dato obtenido se ha utilizado para la finalidad de control de la relación laboral o para una finalidad ajena" (FJ 4).*** *Por este lado,* ***se ha suprimido todo rastro del derecho a conocer el uso y destino de los datos, aunque para alcanzar esa conclusión haya sido preciso, en el trance final, confundir el consentimiento con la información, acertadamente diferenciados en el anterior FJ 3".*** *"Frente a todo lo que impugno y censuro, por tanto, estimo que la recta aplicación de un derecho fundamental como el garantizado en el art. 18.4 CE (RCL 1978, 2836) hubiera comportado, como en el pasado fue argumentado con solvencia jurídica y mesura interpretativa, declarar que* ***no hay una habilitación legal expresa para la omisión del derecho a la información sobre el tratamiento de datos personales en el ámbito de las relaciones laborales; y*** *que tampoco es dable situar su fundamento en el mero interés*

empresario sobre el derecho fundamental a la protección de datos, **la cual se aleja de la tesis esgrimida en la sentencia 292/2000.** El voto particular está en desacuerdo sosteniendo que "*no hay una habilitación legal expresa para la omisión del derecho a la información sobre el tratamiento de datos personales en el ámbito de las relaciones laborales; y que tampoco es dable situar su fundamento en el mero interés empresarial de controlar la actividad laboral a través de sistemas sorpresivos o no informados de tratamiento de datos que aseguren la máxima eficacia en el propósito de vigilancia"*. Voto particular que desde luego recalca lo que viene a cambiar el posterior Reglamento de Protección de Datos de la UE 2016/679, de 27 de abril, el cual entre otras novedades excluye el consentimiento tácito de la nueva regulación, por lo que cabe sospechar un cambio en la interpretación futura de la situación que presenta la Sentencia en cuestión.

El concepto de datos está estrechamente ligado al concepto de la información, y en varios países debido a diferencias de interpretaciones podrían equipararse a la información personal de un individuo, como es el ejemplo de Polonia, que en el art. 51 de su Constitución[10] recoge que nadie puede ser obligado a menos que sea por la Ley a la revelación de su información personal, además, no puede ser almacenada y facilitada a otros…etc. Estableciendo límites al derecho de protección de esa información que han de contenerse en una Ley, concepto regulado en un artículo independiente al artículo que versa sobre el honor y la intimidad personal y familiar y que constituye un derecho autónomo e independiente[11].

---

empresarial de controlar la actividad laboral a través de sistemas sorpresivos o no informados de tratamiento de datos que aseguren la máxima eficacia en el propósito de vigilancia. La lógica por la que ha optado la sentencia de la mayoría, fundada en la más primaria utilidad o conveniencia empresarial, quebranta la efectividad del derecho fundamental del art. 18.4 CE (RCL 1978, 2836) , en su núcleo esencial; confunde la legitimidad del fin (en este caso, la verificación del cumplimiento de las obligaciones laborales a través del tratamiento de datos, art. 20.3 LET [RCL 1995, 997] en relación con el art. 6.2 LOPD) con la constitucionalidad del acto (que exige ofrecer previamente la información necesaria, art. 5 LOPD [RCL 1999, 3058]). Y lo cierto es, sin embargo, que cabe proclamar la legitimidad de aquel objetivo (incluso sin consentimiento del trabajador, art. 6.2 LOPD, como señala la Sentencia aprobada) y, al mismo tiempo, hacer constar que lesiona el art. 18.4 CE (RCL 1978, 2836) la utilización, para ejecutar el acto, de medios encubiertos que niegan al trabajador la información exigible".

[10] Constitución Polaca de 2 de abril de 1997 (Konstutycja Rzeczypospolitej Polski z dnia 2 kwietnia 1997 roku).

[11] Art. 47 de la Constitución Polaca "*Każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym.* **Traducción: *"Cada uno tiene derecho a defender legalmente su vida privada, familiar, honor y buen nombre así como a decidir sobre su vida personal".***

2.La evolución del Derecho Europeo.

A raíz de la revolución de las redes, el Consejo de Europa publica en el **año 1981 el Convenio 108** en el cual estableció una serie de pautas con el fin de *"garantizar, en el territorio de cada Parte, a cualquier persona física sean cuales fuere su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales, concretamente su* ***derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona («protección de datos»)"*** y del que se hace firmante España.

A partir de dicho Convenio se elabora en nuestro país **la LORTAD de 29 de octubre de 1992,** la cual atribuye a la Administración la potestad sancionadora *"que es lógico correlato de su función de inspección del uso de los ficheros, similar a las demás inspecciones administrativas, y que se configura de distinta forma según se proyecte sobre la utilización indebida de los ficheros públicos, en cuyo caso procederá la oportuna responsabilidad disciplinaria, o sobre los privados, para cuyo supuesto se prevén sanciones pecuniarias*[12]*".*

Hay que añadir que, por primera vez, el principio de autonomía de información de un individuo fue formulado y desarrollado por el Tribunal Constitucional Federal alemán en una sentencia de 15 de diciembre de 1983, 1BvR 209/83, donde estableció que "en condiciones de procesamiento moderno de los datos", la Constitución de la República Federal de Alemania protege al individuo contra "la recopilación, uso y transferencia ilimitados de datos personales", así como también la Constitución garantiza "el derecho de una persona a actuar sobre la divulgación y el uso de sus datos personales"[13].

[12] Apartado 7 del preámbulo de la LORTAD, Ley 5/1992.

[13]Traducción de trabajo de Jakub Rzucidlo que cita a su vez al P. Barta, J. Litwiński, Ustawa o ochronie danych osobowych. Komentarz. Warszawa 2013, Komentarz do art . 1 http://www.repozytorium.uni.wroc.pl/Content/52920/09_Jakub_Rzucidlo.pdf Consulta 1.02.2018, 20:00

Posteriormente la Unión Europea, considerando que la integración económica y social resultante del establecimiento y funcionamiento del mercado interior va a implicar necesariamente un aumento notable de los flujos transfronterizos de datos personales entre todos los agentes de la vida económica y social, y que éstos van a experimentar un desarrollo constante, y, en aras de establecer un fortalecimiento de la cooperación entre los Estados miembros, elabora la **Directiva 95/46/CE, de 24 de octubre de 1995.** La misma en su considerando 8 establece como fin primordial:

- eliminar los obstáculos a la circulación de datos personales,

- establecer un nivel igualitario en todos los Estados miembros en cuanto a la protección del tratamiento de los datos.

El considerando octavo subraya que es un **objetivo esencial** para el mercado interior y que no puede lograrse mediante la mera actuación de los Estados miembros dada la gran diferencia de la legislación nacional que aplica cada país. Por ello consideró que es fundamental **coordinar las legislaciones de los Estados miembros para que el flujo transfronterizo de datos personales sea regulado de forma coherente y de conformidad con el objetivo del mercado interior**. Por ello los miembros firmantes tenían que trasponer los principios que marcaba la Directiva a la Legislación interna.

Dicha Directiva supone un cambio en todas las legislaciones de los Estados miembros, y en España deriva en la elaboración de la **LOPD de 13 de diciembre de 1999,** que actualmente se encuentra en vigor hasta la entrada de la nueva legislación que desarrollará el **Reglamento de la Unión Europea 2016/679, de 27 de abril, relativo a las personas físicas en lo que respecta al tratamiento de los datos personales y a la libre circulación de éstos,** y por el que se deroga la Directiva 95/46/CE, cuya

aplicación será directa en todos los países miembros a partir del **25 de mayo del año 2018.**

2.a La Carta de los Derechos Fundamentales de la Unión Europea

La Carta de los Derechos Fundamentales de la Unión Europea fue firmada en el año 2000 en Niza y contiene principios generales que ya venía reconociendo la Convención Europea de Derechos Humanos del año 1950. Es aplicable a todas las instituciones, los órganos, las oficinas y las agencias de la Unión Europea, y los derechos y libertades reconocidos en la misma sólo se pueden limitar respetando el principio de proporcionalidad y siempre que tales limitaciones sean necesarias y respondan a objetivos de interés general reconocidos por la Unión, o ante la necesidad de protección de derechos y libertades de los demás.

El artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea, actualizada en el año 2016, que se contiene en el Título II "Libertades", proclama que "*Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan*" y además que los mismos se "*tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación",* estableciendo como fundamental, en su apartado tercero, la creación de una autoridad independiente para el control de las normas que versen sobre los mismos.

La inclusión del derecho a la protección de datos en la Carta subraya su carácter autónomo e independiente. Como ejemplo ilustrativo, en la reciente Sentencia de 18 de septiembre de 2014 (TEDH 2014, 66) , caso Brunet contra Francia , el TEDH subraya lo siguiente: "***La protección de los datos de carácter personal juega un papel fundamental en el ejercicio del derecho al respeto a la vida privada y familiar consagrado en el artículo 8 del Convenio Europeo de Derechos Humanos.*** *Por tanto, la legislación interna debe crear las garantías adecuadas para impedir cualquier utilización de los datos de carácter personal que no fueran conformes con las garantías previstas en este artículo".* Como podemos ver, el derecho a la protección de datos

personales es un derecho independiente, pero, a su vez está estrechamente vinculado con el respeto a la vida privada y familiar regulado en el art. 8 del CEDH.[14]

Sea como sea, todos los derechos fundamentales están sujetos a límites, e así lo pone de relieve la Sentencia del TJUE (Gran Sala), Dictamen de 26 julio 2017, TJCE 2017\193, en sus considerandos 136 a 140:

"*No obstante, los derechos consagrados en los artículos 7 y 8 de la Carta (LCEur 2007, 2329)* ***no constituyen prerrogativas absolutas****, sino que deben considerarse según su función en la sociedad.*

137. A este respecto, debe asimismo ponerse de relieve que, a tenor del artículo 8, apartado 2, de la Carta (LCEur 2007, 2329) , los datos de carácter personal deben tratarse ***«para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley».***

138. Además, con arreglo al artículo 52, apartado 1, primera frase, de la Carta (LCEur 2007, 2329), ***cualquier limitación del ejercicio de los derechos y libertades reconocidos por ésta deberá ser establecida por la ley y respetar su contenido esencial.*** *Según el artículo 52, apartado 1, segunda frase, de la Carta, dentro del* ***respeto del principio de proporcionalidad, sólo podrán introducirse limitaciones a dichos derechos y libertades cuando sean necesarias y respondan efectivamente a objetivos de interés general reconocidos por la Unión o a la necesidad de protección de los derechos y libertades de los demás.***

139. Cabe añadir que el requisito de que cualquier limitación del ejercicio de los derechos fundamentales deba ser establecida por ley implica que ***la base legal que permita la injerencia en dichos derechos debe definir ella misma el alcance de la limitación del ejercicio del derecho de que se trate****.*

140. En cuanto a la observancia del ***principio de proporcionalidad,*** *la protección del derecho fundamental al respeto de la vida privada en el ámbito de la Unión exige, con arreglo a la jurisprudencia reiterada del Tribunal de Justicia, que las excepciones a la*

[14] Así lo establece también el art. 1.1 de la Directiva 95/46/CE.

protección de los datos personales y las limitaciones de esa protección no excedan de lo estrictamente necesario (sentencias de 16 de diciembre de 2008 (TJCE 2008, 315), Satakunnan Markkinapörssi y Satamedia, C-73/07, EU:C:2008:727, apartado 56; de 8 de abril de 2014 (TJCE 2014, 104) , Digital Rights Ireland y otros, C-293/12 y C-594/12, EU:C:2014:238, apartados 51 y 52; de 6 de octubre de 2015 (TJCE 2015, 324), Schrems, C-362/14, EU:C:2015:650, apartado 92, y de 21 de diciembre de 2016 (JUR 2017, 20668) , Tele2 Sverige y Watson y otros, C-203/15 y C-698/15, EU:C:2016:970, apartados 96 y 103).

141. Para cumplir este requisito, ***la normativa controvertida que conlleve la injerencia debe establecer reglas claras y precisas que regulen el alcance y la aplicación de la medida en cuestión e impongan unas exigencias mínimas****, de modo que las personas cuyos datos se hayan transferido dispongan* ***de garantías suficientes que permitan proteger de manera eficaz sus datos de carácter personal contra los riesgos de abuso.*** *En particular, dicha normativa deberá indicar en qué circunstancias y con arreglo a qué requisitos puede adoptarse una medida que contemple el tratamiento de tales datos, garantizando así que la injerencia se limite a lo estrictamente necesario. La necesidad de disponer de tales garantías reviste especial importancia cuando los datos personales se someten a un tratamiento automatizado. Estas consideraciones son aplicables en particular cuando está en juego la protección de esa categoría particular de datos personales que son los* ***datos sensibles****".*

2.b Jurisprudencia del TEDH

Puesto que España forma parte del CEDH del año 1950, ratificado el 4 de octubre de 1979 (BOE de 10 de octubre de 1979), y ello supone una interpretación de los derechos fundamentales reconocidos por la Constitución Española acorde con el mismo, es relevante abordar un análisis de las sentencias del Tribunal Europeo de Estrasburgo en cuanto a la configuración del derecho a la protección de datos personales. El Convenio Europeo de Derechos Humanos no contempla al derecho a la protección de datos *estricto sensu*, sino que el TEDH considera que el mismo está protegido por el

art. 8.1[15] del mismo, y así viene a confirmar en su reciente jurisprudencia del año 2017 sobre la videovigilancia y la protección de los datos personales, en la que expresa que el término **"vida privada"** "es un **término amplio no susceptible de definición exhaustiva** y que sería demasiado restrictivo limitar la noción de **"vida privada" a un "círculo interno"** en el que el individuo puede vivir **su propia vida personal como él elige** y **excluir de ella completamente el mundo exterior.** El **artículo 8** garantiza así el derecho a la **"vida privada" en sentido amplio,** incluido el derecho a llevar una **"vida social privada",** es decir, **la posibilidad de que el individuo desarrolle su identidad social.** A ese respecto, el derecho en cuestión consagra la posibilidad de acercarse a otros para establecer y desarrollar relaciones con ellos", de modo que además "la noción de "vida privada" puede incluir actividades **o actividades profesionales que tienen lugar en un contexto público"**[16]**.**

Dicha extensión de la vida privada a aspectos sociales queda reflejada en varias sentencias del Tribunal, a saber:

- Caso OF BĂRBULESCU v. ROMANIA, donde el TEDH considera vulnerado el art. 8 del CEDH cuando no se cumpla con un deber de información previa y clara al trabajador de que en la empresa se llevan a cabo controles de correos privados (en los que únicamente el trabajador tiene conocimiento de las contraseñas) de los trabajadores, en los ordenadores destinados únicamente al trabajo de oficina[17].

- En el caso de SÕRO v. ESTONIA considera la vulneración del art. 8.1 de la CEDH en cuanto a la divulgación de datos, que en este caso trataban de propaganda de los nombres de antiguos colaboradores del servicio del KGB, cuando ésta sea desproporcionada al fin que se pretende con la Ley de Divulgación[18]. De modo que se

[15] *"1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia".*

[16] STEDH CASE OF ANTOVIĆ AND MIRKOVIĆ v. MONTENEGRO 70838/13, 28/11/2017, Apartado 41, http://hudoc.echr.coe.int/eng?i=001-178904 Sentencia sobre la instalación de cámaras en un anfiteatro donde se impartían clases de matemáticas. El TEDH considera que no se cumplieron los requisitos para la instalación de las mismas y considera vulnerado el derecho a la privacidad de los alumnos.

[17] STEDH de 5 de septiembre de 2017 Asunto 61496/08, 05/09/2017, apartados 77-81.

[18] STEDH, CASE OF SÕRO v. ESTONIA de 3 de diciembre de 2015, 22588/08, párrafos 61-68.

consideró que dicha ley, al no distinguir los niveles de colaboración con dichos servicios, vulneraba el respeto a la vida privada del demandante, ocasionándole graves daños morales.

- En el caso de Bouchacourt vs Francia, el TEDH considera que un estado ha de proporcionar garantías suficientes contra los usos improcedentes y excesivos[19].
- En el asunto P.G. y J.H. , el Tribunal estimó que el registro de datos y el carácter sistemático o permanente del registro podía hacer que se vulnerase el derecho al respeto de la vida privada incluso si los datos en cuestión eran del dominio público o estaban disponibles de otra manera. Señaló que la grabación de la voz de una persona en un soporte permanente para su análisis posterior perseguía manifiestamente, en combinación con otros datos personales, facilitar la identificación de esta persona. Juzgó, por tanto, que el registro de las voces de los demandantes para dicho análisis ulterior había vulnerado su derecho al respeto de su vida privada[20].

Respecto de conservación de huellas digitales por parte de autoridades del Reino Unido, el Tribunal estima que el carácter general e indiferenciado de la facultad de conservar las huellas dactilares, las muestras biológicas y los perfiles de ADN de las personas sospechosas de haber cometido delitos, pero que no han sido condenadas, no guarda un equilibrio justo entre los intereses públicos y privados que concurren y que el Estado demandado ha superado cualquier margen de apreciación aceptable en la materia. Por tanto, la conservación en litigio se ha de considerar una lesión desproporcionada del derecho de los demandantes al respeto de su vida privada y no puede considerarse necesaria en una sociedad democrática[21].

2.c Art 16 TFUE (antiguo 286 del TCE)

---

[19] STEDH de 17 de diciembre de 2009, párrafo 61.

[20] Sentencia P.G. y J.H. contra Reino Unido (TEDH 2001, 552) , núm. 44787/1998, aps. 59-60, TEDH 2001-IX.

[21] Caso S. y Marper contra Reino Unido. Sentencia de 4 diciembre 2008. TEDH 2008\104 Expositivo 125.

El derecho a la protección de datos que tiene toda persona la incorpora el art.16 del Tratado de Funcionamiento de la Unión Europea, que antiguamente se recogía en el artículo 286 del Tratado de la Comunidad Europea. A partir de ahora constituye la base jurídica para la adopción de normas de protección de datos[22]. Además, su apartado dos hace mención expresa a las normas que han de adoptar los Estados en cuanto a la protección del derecho, así como al establecimiento de unos controles por autoridades de control independientes. Todo ello para garantizar el cumplimiento efectivo de dichas normas.

Artículo 16:

1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.

2. El Parlamento Europeo y el Consejo establecerán, con arreglo al ***procedimiento legislativo ordinario,*** *las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por las instituciones, órganos y organismos de la Unión, así como por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión, y sobre la libre circulación de estos datos. El respeto de dichas normas estará sometido al* ***control de autoridades independientes.***

III. EL NUEVO REGLAMENTO EUROPEO

1. El Reglamento General de Protección de Datos de 27 de abril de 2016

El Nuevo Reglamento General de Protección de datos (en adelante RGPD), que resulta de aplicación directa a partir del 25 de mayo de 2018, es una constatación de un marco normativo cada vez más detallado sobre la materia de protección de datos.

Como las principales novedades de la normativa podemos señalar:

[22] Considerando 10 de la Propuesta de Reglamento del Parlamento Europeo y del Consejo 2012/0011 (COD).

- Una extensión del ámbito territorial. Su aplicación se extiende más allá de la Unión Europea, puesto que, prevé en su artículo segundo que será aplicable al tratamiento de datos personales de residentes en la Unión "**por parte de un responsable o encargado no establecido en la Unión,** cuando las actividades de tratamiento estén relacionadas con la oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si a estos se les requiere su pago, o bien el control de su comportamiento, en la medida en que este tenga lugar en la Unión" (art.3 del RGPD).
- Se amplía la **obligación respecto del deber de informar a los usuarios y clientes** y se obliga a que **el consentimiento del usuario deberá ser siempre explícito**, bajo una declaración o acción afirmativa.
- **La figura del Delegado de Protección de Datos** destaca como importante para las empresas, de modo que debe garantizar auditorías para avalar el cumplimiento del Reglamento, además de tener que informar sobre los incumplimientos.
- Se exigen evaluaciones anteriores al tratamiento en cuanto a la seguridad de determinados datos por parte de los Delegados de Protección de Datos. Los niveles de seguridad han de estar asegurados sobre todo en cuanto a los datos sensibles.
- Las empresas tienen el deber de informar a las Autoridades sobre infracciones cometidas dentro de las mismas, así como sobre los posibles ataques del exterior hacía ficheros que tengan en su posesión (art. 33). Esto puede plantear la cuestión de cuándo se puede considerar que un controlador se ha "enterado" de un incumplimiento. El Grupo Europeo de Protección de Datos del art.29, considera que, un controlador debe considerarse "consciente" cuando tiene un grado razonable de certeza de que ha ocurrido un incidente de seguridad que ha afectado a datos personales comprometidos. Esto dependerá de las circunstancias de la infracción específica. En algunos casos, será relativamente claro desde el principio que ha habido una violación, mientras que, en otros, puede llevar un tiempo establecer si los datos personales se han visto comprometidos. Sin embargo, el énfasis debe estar en la acción inmediata para investigar un incidente para determinar si los datos personales han sido infringidos, y, si es así, para tomar medidas correctivas y notificar si es necesario. Por ejemplo, en el caso de una pérdida de un CD con datos no cifrados, a menudo no es posible determinar si existen personas no autorizadas que obtuvieron acceso al mismo. Sin embargo, tal caso debe notificarse, ya que hay

un grado razonable de certeza de que se ha producido una infracción; el encargado de tratamiento sería consciente de la infracción cuando se dio cuenta de que el CD se había perdido[23].

- Las multas sobre posibles infracciones pueden llegar a alcanzar 200.000.000 €.
- Se elimina a su vez la obligación de inscripción de ficheros, aunque no se exime de llevar el control de los mismos por parte de responsable de tratamiento o delegado de protección de datos (debido a una escasa eficacia de dicha medida).
- Uno de los aspectos más relevantes del Reglamento es **que da mucho más control a los ciudadanos sobre qué permiten o autorizan** que se haga con sus datos.
- Se recomienda determinar la edad para prestar consentimiento para el tratamiento de los datos en 16 años, pero deja al arbitrio de los países miembros la fijación de esta hasta un límite de 13 años (probablemente porque en varios países esa es la edad para consentir determinados actos[24]).
- Aparecen conceptos como seudonimización de datos o principio de minimización de datos (art.4.5 RGPD).
- Se propicia la defensa del derecho a la protección de datos mediante asociaciones y elaboración de códigos de conducta por parte de estas (lo que se pretendía con el art. 27 de la Directiva 95/46/CE).
- Se incentiva a cambios en la normativa laboral en cuanto al consentimiento de los trabajadores para el tratamiento de sus datos.
- Se hace hincapié en la normativa de la Administración Pública en cuanto al tratamiento de los datos.

Por otro lado, y como señala PABLO GARCÍA MEXÍA, el nuevo RGPD deja un amplio margen de desarrollo de Reglamento a los países miembros en materias como:

- Libertad de expresión e información (art. 85 RGPD)
- Acceso público a documentos oficiales (art. 86 RGPD)

[23] Directrices para la notificación de las infracciones art.33 RGPD http://www.agpd.es/portalwebAGPD/canaldocumentacion/docu_grupo_trabajo/wp29/common/Versiones_ingles/20171013_wp250_enpdf.pdf pág.9 Consulta día 15.01.2018, 20:00

[24] En este sentido el legislador polaco decidió fijar la edad en 13 años alegando que es la edad en la que una persona puede decidir sobre su propio dinero por lo que no veía inconveniente fijar la misma en un límite superior.

- Número nacional de identificación (art. 87 RPGD)
- Ámbito laboral
- Fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos (art. 89 RGPD)
- Obligaciones de secreto (art. 90 RGPD)
- Protección de datos de iglesias y asociaciones religiosas (art. 91 RGPD)
- Procesamiento de datos por obligación legal
- Tratamiento realizado en misiones de interés público
- El tratamiento que llevan a cabo los poderes públicos de un determinado Estado.

2.El por qué de la nueva regulación europea.

El considerando primero de la nueva regulación deja claro que el derecho a la protección de datos de las personas físicas es un derecho fundamental. Como tal ha de respetarse e interpretarse, acorde con otros derechos fundamentales contenidos en la normativa europea, de acuerdo con el principio de proporcionalidad.

El Nuevo Reglamento de Protección de Datos 2016/679 UE, de 27 de abril de 2016, en su considerando sexto señala como fundamento principal con el que se desarrolla la nueva normativa "la rápida evolución tecnológica y la globalización". Efectivamente ambas han planteado nuevos retos para la protección de los datos personales.[25]

En la evaluación del funcionamiento de los nuevos instrumentos de la UE en materia de protección de datos (Estrategia Europa 2020), la Comisión realizó consultas sobre el enfoque global en la materia. El resultado mostró que los países están de acuerdo con los principios generales establecidos hasta hoy en día, sobre todo mediante la Directiva 95/46/CE, **pero, es necesario, debido a la magnitud y de la rapidez con la que se desarrolla la tecnología a nivel global, adoptar una mayor seguridad**

[25] La magnitud de la recogida y del intercambio de datos personales ha aumentado de manera significativa con la constante evolución de herramientas tecnológicas, y a su vez supone un cambio en el derecho de la era digital. La tecnología permite que tanto las empresas privadas como las autoridades públicas utilicen datos personales en una escala sin precedentes a la hora de realizar sus actividades. Por otro lado, las personas físicas difunden un volumen cada vez mayor de información personal a escala mundial.

jurídica y la armonización de las normas. Todo ello manteniendo el principio de neutralidad tecnológica[26]. Los grandes operadores económicos insistieron en su preocupación sobre todo por las transferencias de datos al exterior, puesto que las normativas adoptadas en distintos países dificultan considerablemente su funcionamiento,[27] es decir, influyen negativamente en el desarrollo de las empresas y en el comercio en general (desde luego las grandes empresas a nivel internacional tuvieron que ver con la presión ejercitada en este sentido). De modo que era totalmente necesario adoptar normas más armonizadas y más efectivas.

El reglamento deja un margen amplio de desarrollo de la normativa general y sectorial de cada país y, hasta ahora, en España se elaboró un Proyecto de Ley con fecha de 24 de noviembre de 2017[28]. En cuanto a otros países europeos, Alemania modificó su normativa DSG[29] (nuestra LOPD) y ya está en vigor. En Polonia el Proyecto de Ley se elaboró en marzo, el periodo de consultas se cerró el día 13 de octubre de 2017 y la ley aún está pendiente de publicación[30]. En Italia se sigue sin modificar el Código de Protección de datos[31], en Dinamarca las últimas publicaciones son las que se adecuan a

[26] Cristina Cullell March, "El principio de neutralidad tecnológica y de servicios en la UE: la liberalización del espectro radioeléctrico" Artículo: Revista de Internet Dret y Política: "*El principio de neutralidad tecnológica se utilizó por primera vez como principio de regulación el año 1999 en un documento oficial de la Comisión Europea sobre la revisión del marco normativo de las comunicaciones electrónicas.4 Este principio se adoptó como uno de los cinco principales que regían el marco regulador de las comunicaciones electrónicas en la UE. Según este documento, la neutralidad tecnológica supone que la legislación debe definir los objetivos a conseguir sin imponer ni discriminar el uso de cualquier otro tipo de tecnología para conseguir los objetivos fijados.5 El preámbulo de la Directiva Marco 21/2002/CE6 y sobre todo el articulado de la Directiva 2009/140/CE lo incorpora como principio básico de regulación de las comunicaciones electrónicas propias de un entorno convergente, en el cual sectores claramente diferenciados hasta el momento –telecomunicaciones, medios de comunicación y tecnologías de la información– utilizan la misma tecnología para llevar a cabo sus actividades".*Consulta 3.02.2018, 19:00

[27] Informe de la Comisión Europea sobre evaluación del funcionamiento de los instrumentos de la UE en materia de protección de datos, pág. 4.

[28] http://www.congreso.es/public_oficiales/L12/CONG/BOCG/A/BOCG-12-A-13-1.PDF http://www.lamoncloa.gob.es/consejodeministros/Paginas/enlaces/101117enlacedatos.aspx Consulta 02.01.2018

[29]https://www.dsb.gv.at/datenschutz-grundverordnung Consulta 03.03.2018

https://www.parlament.gv.at/PAKT/VHG/XXV/ME/ME_00322/fname_635512.pdf Consulta 04.01.2018

[30] https://www.gov.pl/cyfryzacja/nowe-prawo-ochrony-danych-osobowych Consulta 15.01.2018

https://www.gov.pl/cyfryzacja/dokumenty27 (el preámbulo, el proyecto y la Ley)

la Directiva 95/46/CE[32]. Podríamos decir que únicamente Alemania tiene una Ley adaptada en vigor, y de entre otros países de la UE y del EEE únicamente España y Polonia tienen elaborados los Proyectos de Ley que se adecuan al RGPD.

3.El objeto del nuevo RGPD

En su artículo 1 establece que:

" El presente Reglamento establece las ***normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales*** *y las normas relativas a* ***la libre circulación de tales datos.***

2. El presente Reglamento ***protege los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales".***

Por tanto, se trata de un objeto de doble vertiente, la primera, protección de persona física (quedan por tanto excluidas las personas jurídicas) en lo que se refiere al tratamiento de los datos personales, así como protección de la libre circulación de los mismos. En su considerando 101 se indica que los flujos transfronterizos de datos personales son necesarios para la expansión del comercio y la cooperación internacionales, cuyo aumento plantea nuevos retos en cuanto a la protección de los mismos. De modo que se pretende elaborar una normativa que no obstaculice dicha circulación y facilite el flujo económico, pero a su vez tenga por objetivo la seguridad.

El legislador se da cuenta a su vez de los problemas que se plantean a nivel de transferencias de datos a terceros países que no pertenecen a la UE. En este sentido se intenta adoptar acuerdos como por ejemplo la Decisión de Ejecución (UE) 2016/1250,

[31] No existe una adaptación al RGPD. En Italia entre otras cosas se elaboró un código de buena conducta en la utilización de datos personales del 13 de octubre de 2015, en adaptación del art.27 de la Directiva 95/46/CE. http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/4298343 Consulta 1.02.2018

[32] https://www.datatilsynet.dk/english/the-act-on-processing-of-personal-data/read-the-act-on-processing-of-personal-data/compiled-version-of-the-act-on-processing-of-personal-data/ Consulta 04.01.2018

de 12 de julio, sobre la adecuación de la protección proporcionada por el acuerdo Privacy Shield (conocido como "escudo privacidad entre Europa y Estados Unidos")[33].

Es de subrayar el apartado dos del mismo artículo, puesto que se indica la protección de los datos claramente como un derecho fundamental.

La normativa se aplica entonces a las personas físicas, independientemente de su nacionalidad o de su lugar de residencia. Es decir, que cualquier ciudadano, aunque no perteneciente a los países de la UE o del EEE, puede invocar su derecho fundamental a la protección de datos.

Asimismo, puede apreciarse que el legislador fija, como la esencia de la norma, la tutela del derecho fundamental a la protección de datos en tanto que derecho instrumental para el sistema de derechos fundamentales y libertades públicas, aunque sin olvidar su estrecha relación con los derechos al honor y a la intimidad personal y familiar. Una definición un tanto distinta si la comparamos con la LOPD 15/1999, que proclama en su art.1: *"La presente Ley Orgánica tiene por objeto garantizar y proteger, en lo que* ***concierne al tratamiento de datos personales,*** *las libertades públicas y los derechos fundamentales de las personas físicas,* ***y especialmente de su honor e intimidad personal y familiar".***

Por otro lado, el legislador pretende garantizar la libre circulación de los mismos, como destaca también en el considerando 13, de modo que se asegura dotar de seguridad jurídica y de transparencia a los operadores económicos de los mercados (aplicable a empresas grandes, medianas y pequeñas, dotando el sistema de una supervisión coherente a nivel europeo.

4.Estructura del RGPD.

El Reglamento Europeo de Protección de Datos (en adelante RGPD) contiene 173 considerandos y 99 artículos y está dividido en 11 capítulos:

• Capítulo I: Disposiciones generales (artículos 1 a 4)

[33] https://www.boe.es/doue/2016/207/L00001-00112.pdf Consulta 10.01.2018

• Capítulo II: Principios (artículos 5 a 11)
• Capítulo III: Derechos del interesado (artículos 12 a 23)
• Capítulo IV: Responsable y procesador (artículos 24 a 43)
• Capítulo V: Transferencias de datos personales hacia o desde terceros países u organizaciones internacionales (artículos 44 a 50)
• Capítulo VI: autoridades de supervisión independientes (artículos 51 a 59)
• Capítulo VII: Cooperación y coherencia (artículos 60 a 76)
• Capítulo VIII: Recursos, responsabilidad y sanciones (artículos 77 a 84)
• Capítulo IX: Requisitos para situaciones especiales de procesamiento (artículos 85 a 91)
• Capítulo X: actos delegados y de ejecución (artículos 92 a 93)
• Capítulo XI: Disposiciones finales (artículos 94 a 99)

5.Ámbito de aplicación material.

La aplicación del RGPD abarca toda la clase de ficheros sobre tratamiento de datos de las personas físicas (art. 2 RGPD)[34], pero no se aplicará a ficheros o conjuntos de ficheros, así como sus portadas, que no estén estructurados con arreglo a criterios específicos.

Se excluye su aplicación en los siguientes supuestos:

a) en el ejercicio de una actividad no comprendida en el ámbito de aplicación del Derecho de la Unión;

b) por parte de los Estados miembros cuando lleven a cabo actividades comprendidas en el ámbito de aplicación del capítulo 2 del título V del TUE;

[34] Considerando 15 del Reglamento La protección de las personas físicas debe aplicarse al tratamiento automatizado de datos personales, así como a su tratamiento manual, cuando los datos personales figuren en un fichero o estén destinados a ser incluidos en él.

c) efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas[35];

d) por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención.

6. Conceptos y definiciones básicas.

El RGPD introduce una serie de definiciones y conceptos básicos que incorpora en los considerandos y en los artículos de desarrollo (art. 4 del RGPD). Entre ellos vamos a mencionar algunos que nos resultan más relevantes a efectos del presente trabajo. En el artículo 4 se contienen definiciones como:

1)Los datos personales. Son toda información sobre una **persona física identificada o identificable** (es decir, que podemos aplicar dicho concepto a una posible identificación futura), es decir, **interesado.** Vemos que es un concepto muy similar al que había establecido ya tanto la Directiva como el art. 5 f) del RLOPD[36].

2)El interesado. Es toda persona identificada o que se pueda identificar directa o indirectamente (mediante un nombre, un número de identificación, datos de localización o mediante elementos de la identidad física, genética, psíquica, económica, cultural, o social). Con dicha definición podemos concluir que se trata de una serie de parámetros que permitan atribuirse a una persona identificada o a una serie de parámetros que permitan identificarla.

[35] Existen en cuanto a las actividades domésticas unas recientes conclusiones de Abogado General, de 1 de febrero de 2018 en el Asunto C-25/17, Tietosuojavaltuutettu contra Jehovan todistajat, que aluden que la actividad de testigos de Jehová o "predicadores de puerta en puerta", trasciende de mero uso doméstico de los datos, puesto que se reparten por zonas a los predicadores y se facilitan datos sobre la situación religiosa (además sensibles) a autoridades superiores en dicha comunidad. http://curia.europa.eu/juris/document/document.jsf?text=protecci%25C3%25B3n%2Bde%2Bdatos&docid=198949&pageIndex=0&doclang=es&mode=req&dir=&occ=first&part=1&cid=470972#ctx1

[36] Datos de carácter personal: Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables.

3)Seudonimización de los datos: el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable. Es decir, que se trata de utilización de seudónimos en vez de nombres reales de las personas, teniendo seleccionada toda la información relativa a la misma en ficheros que sean independientes y que tengan un nivel de seguridad adecuado.

4)Consentimiento del interesado: Toda manifestación de voluntad libre, **específica, informada e inequívoca** por la que el interesado acepta, ya sea mediante una declaración o **una clara acción afirmativa**, el tratamiento de datos personales que le conciernen. Se deduce que no cabe entonces un consentimiento tácito de la persona puesto que el término inequívoco viene reforzado con una acción clara y afirmativa. El concepto fue recogido por la RLOPD en su art. 5, según el cual "el consentimiento es toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen", pero admitía consentimiento tácito en su art. 14, cuando el titular de los datos no se oponía al tratamiento solicitado (no aplicable a datos sensibles que el RGPD recoge en su art. 9, donde prohíbe el uso de dichos datos). En cuanto al consentimiento, además, se establece en el art.7.3 del RGPD que la retirada del mismo debe ser igual de fácil como darlo. De modo que cabe interpretar que, si el usuario ha prestado su consentimiento vía formulario electrónico, pueda hacerlo mediante la misma vía.

7.Los principios de protección de datos que se contemplan en la nueva normativa.

En palabras de PUYOL MONTERO, podemos entender por principios de la protección de datos "un conjunto de reglas que determinan cómo se deben recoger, tratar y ceder los datos de carácter personal a los efectos de garantizar la intimidad y

demás derechos fundamentales de los titulares de los datos, los consumidores o usuarios y en definitiva, los ciudadanos"[37].

En el nuevo Reglamento General de Protección de Datos 2016/679 se encuentran recogidos en el capítulo II, artículos 5º al 11º, y refieren al tratamiento, la licitud, las condiciones en las que debe recogerse el consentimiento del interesado y los requisitos aplicables al mismo, la recogida de los datos de los menores, categorías especiales de datos personales, datos concernientes a infracciones de naturaleza penal y tratamientos que no requieren una especial identificación.

La normativa en cuestión habla de *"los principios de tratamiento leal y transparente"*, información al interesado, de la existencia de la operación de tratamiento y sus fines (considerando 60), e introduce un deber de proporcionar la información complementaria para garantizar a los mismos, además de, "*informar al interesado de la existencia de la elaboración de perfiles y de las consecuencias de dicha elaboración. Si los datos personales se obtienen de los interesados, también se les debe informar de si están obligados a facilitarlos y de las consecuencias en caso de que no lo hicieran.* ***Dicha información puede transmitirse en combinación con unos iconos normalizados que ofrezcan, de forma fácilmente visible, inteligible y claramente legible, una adecuada visión de conjunto del tratamiento previsto***. *Los iconos que se presentan en formato electrónico deben ser legibles mecánicamente".*

a. Sustitución del principio de calidad de los datos por los principios del art. 5 del RGPD.

El artículo 4 de la actual LOPD 15/1999, de 13 de diciembre, recoge en su título II, y bajo el nombre de "Principios de protección de datos", el principio de calidad de datos por el que estos deben ser *"adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido",* por lo que *"no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos".* Además de ello, tendrán que ser exactos y veraces, por lo que han de estar actualizados y, de no ser así, tendrá que

[37] PUYOL MONTERO.J, "Los principios del Derecho a la Protección de Datos" en "Reglamento General de Protección de Datos", pp. 135-141, Director : Piñas Mañas J.L, Ed. REUS, Madrid 2016.

procederse a su cancelación de oficio y reemplazados por los datos rectificados. De igual modo hay que proceder a cancelar los datos si dejan de ser necesarios para el fin para el cual hubiesen sido recogidos, quedando prohibida la conservación de estos, salvo en los casos de los valores históricos, estadísticos o científicos regulados por la correspondiente legislación. Se establece asimismo en el apartado sexto un derecho de acceso a los mismos y se prohíbe la recogida por medios fraudulentos, desleales o ilícitos.

Es importante aclarar que los datos, según la LOPD, tienen que ser adecuados, es decir, que se recojan acorde a la finalidad con la que se van a tratar para que dicho tratamiento sea lícito. Dicho de otra manera, si el objetivo de recoger los datos es, por ejemplo, emitir una factura de teléfono, no sería adecuado pedir al interesado los datos relativos a la vida familiar del mismo (si tiene hijos, etc.), un dato adecuado sería el número de teléfono, la dirección, etc. Ahora bien, existe la posibilidad de que un tratamiento de datos sea lícito en un principio por respetar dichas exigencias y que con el paso de tiempo deje de serlo, ya que los datos pueden dejar de ser necesarios para el fin con el que fueron recogidos en cualquier momento de tratamiento de estos[38]. El TEDH ha declarado, en su Sentencia de 18 de septiembre de 2014 (TEDH 2014, 66) , caso Brunet contra Francia, lo siguiente en cuanto al contenido del art. 8 de la Carta de Derechos Fundamentales: *"(...) la legislación interna debe crear las garantías*

[38]STS 210/2016 de 5 abril. RJ 2016\1006 (FJ,5) párrafo 13: *"El factor tiempo tiene una importancia fundamental en esta cuestión, puesto que el tratamiento de los datos personales debe cumplir con los requisitos que determinan su carácter lícito y, en concreto, con los principios de calidad de datos(adecuación, pertinencia, proporcionalidad y exactitud), no solo en el momento en que son recogidos e inicialmente tratados, sino durante todo el tiempo que se produce ese tratamiento. Un tratamiento que inicialmente pudo ser adecuado a la finalidad que lo justificaba puede devenir con el transcurso del tiempo inadecuado para la finalidad con la que los datos personales fueron recogidos y tratados inicialmente, y el daño que cause en derechos de la personalidad como el honor y la intimidad, desproporcionado en relación al derecho que ampara el tratamiento de datos. En este sentido, el apartado 93 de la STJUE del caso Google declaraba que «incluso un tratamiento inicialmente lícito de datos exactos puede devenir, con el tiempo, incompatible con dicha Directiva cuando estos datos ya no sean necesarios en relación con los fines para los que se recogieron o trataron. Este es el caso, en particular, cuando son inadecuados, no pertinentes o ya no pertinentes o son excesivos en relación con estos fines y el tiempo transcurrido»".*

adecuadas para impedir cualquier utilización de los datos de carácter personal que no fueran conformes con las garantías previstas en este artículo. La legislación interna debe garantizar que estos datos son pertinentes y no excesivos en relación a ***la finalidad*** *para la que fueron registrados, y que se conservan de forma que permita la identificación de las personas por un tiempo* ***que no exceda el necesario a los fines para los que fueron registrados****".*

En palabras de REBOLLO DELGADO y SERRANO PÉREZ, "se trata de una finalidad explícita, determinada y legítima, fijada con anterioridad a la recogida de datos y además ha de constar si se trata de un fichero de titularidad pública o privada"[39].

Finalidad explícita que viene ahora reafirmada por el nuevo RGPD en su Capítulo II, titulado "Principios", por lo que cabe interpretar que todos los artículos (del 5 al 11) contienen los principios que han de informar el resto del Reglamento. Sin embargo, al hacer la lectura de estos, podemos observar que el núcleo se contiene en el art. 5º y los restantes constituyen una concreción.

El principio de transparencia: contenido en el considerando 39 del Reglamento, exige que toda información y comunicación relativa al tratamiento de dichos datos **sea fácilmente accesible y fácil de entender**, y que se **utilice un lenguaje sencillo y claro.** Dicho principio se refiere en particular a la información de los interesados sobre la **identidad del responsable** del tratamiento y **los fines** del mismo y a la información añadida para garantizar un **tratamiento leal y transparente** con respecto a las personas físicas afectadas y a su **derecho a obtener confirmación y comunicación de los datos personales** que les conciernan que sean objeto de tratamiento. Las personas físicas deben tener **conocimiento de los riesgos, las normas, las salvaguardias y los derechos relativos al tratamiento de datos personales así como del modo de hacer valer sus derechos en relación con el tratamiento.**

1)Limitación de la finalidad: Se trata de un límite al principio de finalidad de la recogida de los datos, de modo que se pueden tratar los datos con fines de archivo en

[39] REBOLLO DELGADO.L, SERRANO PÉREZ.MM, "Manual de Protección de Datos", p.144., pár.3. 2º ed. Dykinson S.L (UNED), Madrid, 2017

interés público, fines de investigación científica e histórica o fines estadísticos (no se consideran incompatibles con los fines iniciales con los que fueron recogidos)

2)Principio de minimización de los datos: los datos tienen que ser "mínimos" o adecuados, o limitados a lo necesario en relación con el fin con el que se recogen (lo que la LOPD definía como el principio de adecuación de los datos).

3)Principio de exactitud de los datos: tienen que ser exactos y, si fuera necesario, actualizados. A tal fin se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales **que sean inexactos con respecto a los fines para los que se tratan.**

4)Principio de limitación del plazo de conservación: los datos pueden mantenerse (de tal forma que se permita la identificación de una persona) durante no más tiempo del necesario para los fines del tratamiento. Sólo podrán exceder de este periodo si se tratan con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos.

5)Principio de integridad y de confidencialidad de los datos: deben ser tratados de tal manera que se garantice una seguridad adecuada de los mismos. El responsable tendrá que adoptar la protección contra el tratamiento no autorizado o ilícito y contra la pérdida de datos, su destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas.

6)Principio de responsabilidad proactiva: el responsable de tratamiento será responsable del cumplimiento de los principios mencionados y además tendrá que demostrar que adoptó las medidas correspondientes para dicho cumplimiento.

Para la mejor interpretación del artículo 5 tenemos que tener en cuenta el considerando 39: Todo tratamiento de datos personales debe ser **lícito y leal**. Para las personas físicas **debe quedar totalmente claro que se están recogiendo, utilizando, consultando o tratando de otra manera datos personales que les conciernen**, así como la medida en que dichos datos son o serán tratados.

En particular, los **fines** específicos del tratamiento de los datos personales deben ser **explícitos y legítimos,** y **deben determinarse en el momento de su recogida**. Los datos personales deben ser **adecuados, pertinentes y limitados a lo necesario** para los fines para los que sean tratados. Ello requiere, en particular, garantizar que se **limite a un mínimo estricto su plazo de conservación.** Los datos personales solo deben tratarse si la finalidad del tratamiento no pudiera lograrse razonablemente por otros medios. Para garantizar que los datos personales no se conservan más tiempo del necesario, el responsable del tratamiento **ha de establecer plazos para su supresión o revisión periódica.** Deben tomarse todas las medidas razonables para garantizar que se rectifiquen o supriman los datos personales que sean inexactos. Los datos personales deben tratarse de un modo que garantice una **seguridad y confidencialidad adecuadas inclusive para impedir el acceso o uso no autorizados y del equipo utilizado en el tratamiento.**

b. El art. 6 referente a la licitud del tratamiento

Para que el tratamiento sea lícito tiene que cumplir al menos las siguientes condiciones:

a) Cuando el responsable dispone de consentimiento por parte del interesado, para el tratamiento de sus datos personales para uno varios **fines específicos**

b) No dispone del consentimiento expreso pero el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de éste de medidas precontractuales.

c) No dispone del consentimiento, pero el tratamiento es legal porque es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento

d)No dispone del consentimiento, pero el tratamiento es necesario para proteger los intereses vitales del interesado o de otra persona física

e) No dispone de consentimiento, pero el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable de tratamiento

f) No dispone de consentimiento, pero el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable de tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.

Por tanto, podemos ver que, mientras el apartado a) constituye la regla principal en cumplimiento de los principios contenidos en el artículo anterior, el resto de los apartados constituyen las excepciones a la regla de un consentimiento explícito, inequívoco e informado[40].

Ídem para el apartado cuarto (art.6.4) de dicho artículo, que permite la recogida de los datos para un fin distinto del fin para el cual fueron recogidos, observando siempre los siguientes elementos:

a) Cualquier relación entre los fines para los cuales se hayan recogido los datos personales y los fines del tratamiento ulterior previsto

b) El contexto en el cual se hayan recogido los datos personales, en particular por lo que respecta a la relación de los interesados y el responsable de tratamiento.

c) La naturaleza de los datos personales, en concreto cuando se traten categorías especiales de datos personales, de conformidad con el art. 9, o datos personales relativos a condenas e infracciones penales, de conformidad con el art. 10.

d) Las posibles consecuencias para los interesados del tratamiento ulterior previsto

e) La existencia de garantías adecuadas, que podrán incluir cifrado y seudonimización.

De manera que sí es posible un tratamiento posterior con un fin distinto para el cual los datos fueron recogidos, pero atendiendo a las circunstancias enumeradas en el apartado cuarto del artículo sexto.

[40] En el mismo sentido ADUSARA VARELA,B. ·"Consentimiento" en "Reglamento General de Protección de Datos", Coordinador PIÑAR MAÑAS J., pág.158. *"No estamos de acuerdo con este enfoque, pues se pone al mismo nivel la regla y las excepciones, y creemos que ha de destacarse , por encima de todo, el principio de libertad y autodeterminación respecto de los propios datos".* Ed. REUS, Madrid, 2016.

c. El consentimiento.

El art. 7 del RGPD recoge "Condiciones para el consentimiento", sin perjuicio de que su definición se establece en el art. 4, apartado 11: "el consentimiento es toda manifestación de voluntad **libre, específica, informada e inequívoca** pudiendo ser una declaración o una acción afirmativa". Por tanto, podemos decir, que un consentimiento para su validez tiene que cumplir, además, con las condiciones previstas en el art. 7, el cual estipula lo siguiente:

En su apartado primero precisa que, **si se trata de un tratamiento basado en el consentimiento** (se excluyen por lo tanto las excepciones del art.6), el responsable debe ser capaz de demostrar que aquel consintió el tratamiento de datos personales. Es lógico que no se requiera dicha prueba de consentimiento en los supuestos de excepciones puesto que, de antemano, no sería posible. Se requiere entonces una prueba contundente por parte de un responsable del tratamiento, sin la cual no se daría la condición de un consentimiento. La prueba constituye pues una *conditio sine qua* non para un consentimiento válido del interesado. Ello supone un reforzamiento, sobre todo en los casos donde un consentimiento se da mediante una declaración telefónica o mediante medios electrónicos, donde la facilidad de una posible "desaparición" de ficheros es muy alta.

En su apartado segundo, se especifica la opción de un **consentimiento manifestado mediante declaración escrita,** que, además, incluye "otros asuntos" (se puede interpretar de manera que el consentimiento se recoge para un fin determinado, pero conlleva, además, otro tipo de fines no relacionados necesariamente con el fin principal). **La solicitud de dicho consentimiento se presentará de tal forma que se distinga claramente de los demás asuntos, de forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo.** Se incluye pues una regla implícita por la cual, si no se cumple con alguno de estos requisitos, tampoco estaríamos ante un consentimiento válido, puesto que se ve frustrada la información previa y por tanto no se cumplen las condiciones.

En este sentido, ADUSARA VARELA opina que el apartado segundo no se refiere a condiciones de consentimiento, sino a la prueba de que éste se dio, y que se dio, cumpliendo las condiciones esenciales que debe tener para que sea válido[41].

En el apartado tercero se establece la posibilidad de la retirada de consentimiento en cualquier momento y un **deber de informar de dicha posibilidad**, además de que la facilidad para retirarlo tiene que ser la misma como para darlo, es decir que si consentimos mediante un formulario o por teléfono tiene que existir igual modo de retirar dicho consentimiento. Por tanto, si no cumplimos con el deber de informar sobre la retirada de la aceptación, o no cumplimos con un medio de fácil acceso para poder realizarlo, tampoco estaríamos ante un consentimiento válido.

Y, finalmente, en su apartado cuarto establece una condición por la cual el consentimiento ha de ser libremente prestado. Para la determinación de si fue libremente prestado se tendrá en cuenta, entre otras cosas, si la ejecución del contrato, incluida la prestación de servicio, se supedita al consentimiento al tratamiento de datos personales que no son necesarios para la ejecución de dicho contrato.

Dicho artículo séptimo debe interpretarse acorde con el considerando 32: El consentimiento debe darse mediante un **acto afirmativo claro** que refleje una **manifestación de voluntad libre, específica, informada, e inequívoca** del interesado **de aceptar el tratamiento** de datos de carácter personal que le conciernen, como una **declaración por escrito**, inclusive **por medios electrónicos**, o una **declaración verbal**.

Aquí el Reglamento hace una recomendación de un acto afirmativo claro, por ejemplo:

- marcar una casilla de un sitio web en internet
- escoger parámetros técnicos para la utilización de servicios de la sociedad de la información, o
- cualquier otra declaración o conducta que indique claramente en este contexto que el interesado acepta la propuesta de tratamiento de sus datos personales.

[41] ADUSARA VARELA, B.” Consentimiento” en “Reglamento General de Protección de Datos”, pág.160. Ed. Reus, 2016

Por tanto, **el silencio, las casillas ya marcadas o la inacción no deben constituir consentimiento** (se excluye la posibilidad que se admitía mediante consentimiento inequívoco y que se entendía como aquel que puede deducirse por una actuación u **omisión** que presupone la existencia de tal consentimiento[42]).

El consentimiento **debe darse para todas las actividades de tratamiento realizadas con el mismo o los mismos fines**. Cuando el tratamiento tenga **varios fines, debe darse el consentimiento para todos ellos**.

Si el consentimiento del interesado **se ha de dar a raíz de una solicitud por medios electrónicos, la solicitud ha de ser clara, concisa y no perturbar innecesariamente el uso del servicio para el que se presta.** Un matiz aparte para los medios electrónicos que constituye un plus en cuanto a la claridad y concisión de la información.

Un artículo aparte, aunque también se trata de consentimiento, se dedica al consentimiento de los niños (art. 8) en relación con los servicios de la sociedad de la información, donde se establece la edad recomendable de 16 años para la validez del tratamiento de los datos (si son menores necesitan de consentimiento de los padres o de un tutor). Recomendación y no obligación, puesto que el Reglamento deja la vía libre para que los Estados miembros puedan fijar los límites por debajo de dicha edad, siempre que ésta no sea inferior a 13 años.

Se impone además una obligación al responsable de tratamiento, dentro de lo razonable, para que verifique la veracidad del consentimiento prestado por el padre o tutor. En cierto sentido, si se trata de servicios de sociedad de información, esta obligación supone para el responsable de tratamiento, intentar asegurarse con quién está celebrando un contrato. Debido a que son contratos celebrados a distancia, siempre existe la incertidumbre en cuanto a la identidad de la otra parte.

8.Tratamiento de categorías especiales de datos personales.

[42]ANDREU MARTÍNEZ M.B; PLANA ARNALDOS M.C. "La protección de los Datos Personales en Internet ante la Innovación Tecnológica" Coordinador: VALERO TORRIJOS.J ,pág.139. Ed. Thomson Reuters Ardanzadi, Navarra 2013.

El artículo 9 establece una regla general de prohibición de tratamiento de los llamados datos sensibles como son:

- datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, ~~y~~

- **el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física** (una de las novedades que no incluía la normativa anterior), y

- datos relativos a la salud o datos relativos a la vida sexual o las orientaciones sexuales de una persona física.

Se establecen a su vez excepciones a dicha prohibición cuando:

Se dispone del consentimiento explícito del interesado para dichos fines.

b) En caso de cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social, siempre acorde a las Leyes.

c) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento;

d) Se traten por una fundación, una asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que el tratamiento se refiera exclusivamente a los miembros actuales o antiguos de tales organismos o a personas que mantengan contactos regulares con ellos en relación con sus fines y siempre que los datos personales no se comuniquen fuera de ellos sin el consentimiento de los interesados;

e) datos personales que el interesado ha hecho manifiestamente públicos (en este sentido, y como subraya ADUSARA VARELA, podríamos referirnos a un consentimiento tácito o una “clara acción afirmativa”).

f) el tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial;

g) el tratamiento es necesario por razones de un interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado;

h) el tratamiento es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social (cuando se traten bajo secreto profesional o bajo una norma).

i) el tratamiento es necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios,

j) el tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos,

Se deja abierta la posibilidad de que los Estados introduzcan condiciones adicionales o limitaciones con respecto de tratamiento de datos genéticos, datos biométricos o datos relativos a la salud.

Se establece en el art. 10 un especial reforzamiento en cuanto al tratamiento de los datos en el ámbito penal (condenas e infracciones o medidas de seguridad conexas, registros completos de condenas penales). El tratamiento en este ámbito habrá que hacerse bajo la supervisión de autoridades públicas o cuando lo autorice el Derecho (sea de la Unión sea de los Estados).

Por último, bajo el epígrafe de "principios" se establece una exención de obligaciones contenidas en los arts. 15-20 (acceso, rectificación, olvido…) en los casos en los que se traten datos que no requieren (o que antes requerían pero se transforman en datos que no requieren) la identificación del interesado.

9.Derechos del interesado y obligaciones del responsable.

Los artículos 12-20 constituyen los derechos de los interesados, así como las obligaciones que suponen a su vez para los responsables de tratamiento.

9.1 Las obligaciones del responsable. El deber de información.

El contenido esencial del derecho fundamental a la protección de datos es la información al interesado sobre qué se está realizando el tratamiento de estos[43]. De modo que, en palabras de HERNANDEZ CORCHETE, "el poder de disposición que un individuo tiene sobre sus datos personales se manifiesta de modo principal en su capacidad para consentir o rechazar un tratamiento de los mismos, decisión que sólo es posible si se le informa previamente de los caracteres definitorios de aquel, sin embargo puede ser limitado por ley"[44].

Para facilitar a los interesados el acceso y el cumplimiento de sus derechos, en virtud del principio de transparencia (en forma clara concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo) el responsable de tratamiento tiene que ajustarse a las siguientes medidas:

1) En caso en el cual se obtenga el consentimiento directamente del interesado:

[43] STC 292/2000, de 30 de noviembre, FJ *6 "(...) pero ese poder de disposición sobre los propios datos personales nada vale si el afectado desconoce qué datos son los que poseen los terceros, quiénes lo poseen, y con qué fin"*

[44] HERNÁNDEZ CORCHETE, J.A "Transparencia en la información al interesado del tratamiento de sus datos personales y en el ejercicio de sus derechos" en "Reglamento General de Protección de Datos", Coordinador: PIÑAR MAÑAS J.L, pág.214, Ed.Reus, Madrid, 2016

- En el momento de la recogida tiene que tomar las medidas oportunas para facilitar al interesado **toda la información** relacionada con[45]:

  a) La identidad y los datos de contacto de responsable y, en su caso, de su representante

  b) Los datos de contacto del delegado de protección de datos en su caso (la figura del DPD introducida por el Reglamento)

  c) Los fines de tratamiento a que se destinan los datos personales y la base jurídica de tratamiento

  d)Los intereses legítimos del responsable o de un tercero

  e) Posibles transferencias a terceros países u organizaciones internacionales y si dichos destinos son adecuados a juicio de la Comisión o indicar garantías adecuadas o apropiadas y a los medios para obtener una copia de estas o al hecho de que se hayan prestado.

  f) El plazo durante el que se conservan los datos o criterios para determinar el mismo

  g) El derecho de acceso, rectificación o supresión o la limitación de su tratamiento o a oponerse al mismo, así como el derecho a la portabilidad de datos

  h) La posibilidad de retirada de consentimiento

  i) Derecho a presentar una reclamación ante una autoridad de control

  j) Si la comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir un contrato, y si el interesado está obligado a facilitar los datos personales y está informado de las posibles consecuencias en el caso de que no los facilite

  k) De la existencia de decisiones automatizadas, incluida la elaboración de perfiles

[45] Estamos hablando de un numerus clausus a diferencia de la redacción abierta que contenía la Directiva utilizando la palabra “al menos”.

l) Si existen otros fines distintos del fin para el cual se recogen los datos y proporcionar la información sobre los mismos

2) Para el caso en el que los datos no se han obtenido del interesado se proporcionará la misma información que se menciona anteriormente como máximo dentro de 1 mes desde la obtención de dichos datos y además, tendrá que indicar la fuente de la que proceden (incluidas las fuentes de acceso público), a excepción de que el interesado ya disponga de dicha información, o su comunicación resulte imposible, la obtención o la comunicación esté expresamente prevista por la Ley o cuando los datos tienen carácter confidencial (obligación de secreto profesional).

Existen por tanto dos momentos en los que el responsable de tratamiento está obligado a informar. Uno ex ante y otro post a la recogida de datos (en plazo de 1 mes).

Dichas obligaciones podrán ser limitadas a través de la legislación interna de los Estados, pero sin desvirtuar su contenido y cuando ello sea necesario en una sociedad democrática, teniendo en cuenta la seguridad del Estado, la defensa o la seguridad pública, persecución de delitos o la ejecución de sanciones penales, objetivos de interés público, protección e independencia judicial, prevención, investigación de normas deontológicas, en función de supervisión, inspección o reglamentación "*incluso ocasionalmente",* con el ejercicio de autoridad pública, ejecución de demandas civiles[46]. Todo ello bajo un procedimiento que tiene que contener dicha Ley, es decir, que no basta elaborar una Ley para limitar dichos derechos, sino que ésta tiene que contener como mínimo las garantías o "justificaciones" contenidas en el apartado 2 del artículo 23.

Sea como sea, y aunque se imponga que se haga mediante ley, el legislador comunitario deja un margen muy flexible a la posibilidad de limitación de derechos u obligaciones que enumera, estableciendo incluso la limitación del artículo 5, es decir, el artículo "estrella" que contiene los principios rectores de dicha estructura normativa.

[46] Art. 23 RGPD

9.2 Los derechos del interesado:

1) derecho de acceso (art.15): comprende el derecho del interesado a obtener una confirmación por parte del responsable de si se están tratando o no sus datos personales (con lo cual a la vez constituye una obligación al responsable de responder al que formula la petición) y si la respuesta resulta afirmativa el responsable está obligado a proporcionar los fines con los que se tratan dichos datos, las categorías de los mismos, a quién se comunicaron o a quien serán comunicados, el plazo de conservación o los criterios para determinar dicho plazo, la posibilidad de solicitar la rectificación, supresión, oposición o limitación del tratamiento de los datos, el derecho de presentar la reclamación ante una autoridad competente, la información sobre el origen de los mismos y sobre la existencia de decisiones automatizadas, y el derecho a obtener una copia gratuita de los datos en cuestión (las demás copias pueden cobrarse en concepto del canon administrativo). Es un derecho que constituye un contenido esencial del derecho a la protección de datos, puesto que una persona, sin poder acceder a la información que posee un responsable sobre ella, difícilmente podría ejercitar el resto de los derechos relacionados con la defensa de sus datos[47].

2)derecho de rectificación: Comprende el derecho del interesado a que sus datos sean exactos o completos. El responsable está obligado a rectificar los mismos y a admitir declaraciones adicionales para completar los datos.

3)derecho de supresión: Es llamado derecho al olvido de un individuo. Se determina mediante el Reglamento una enumeración las circunstancias en las que el responsable tiene una obligación de suprimir los datos **sin dilación indebida**:

- cuando cese el fin o fines con los que fueron recogidos o tratados o no se los trate de otro modo;

[47] En este sentido se pronunció el TJUE en su Sentencia Rotterdam vs. Rijkeboer, Asunto C-553/07, párrafo 51. *"El citado derecho de acceso es indispensable para que el interesado pueda ejercer los derechos que se contemplan en el artículo 12, letras b) y c), de la Directiva, a saber, en su caso, cuando el tratamiento no se ajuste a las disposiciones de la misma, obtener del responsable del tratamiento de los datos, la rectificación, la supresión o el bloqueo de los datos [letra b)], o que proceda a notificar a los terceros a quienes se hayan comunicado los datos, toda rectificación, supresión o bloqueo efectuado, si no resulta imposible o supone un esfuerzo desproporcionado [letra c)]".*

-cuando el interesado retire el consentimiento (se exceptúan casos de excepciones previstas en el art. 6)

-cuando el interesado ejercite el derecho de oposición (y no se den excepciones legales)

-cuando los datos se traten de manera ilícita

-cuando así lo establezca la Ley

-cuando los datos fueran recogidos de un menor

-cuando haya hecho públicos los datos personales y esté obligado a retirarlos a causa de los supuestos anteriores, adoptará medidas razonables para que se supriman los posibles enlaces de acceso a los mismos (o a su copia).

Sin embargo, el Reglamento en el apartado 3 del art.17 establece **excepciones o límites al derecho a la supresión** (o al olvido) cuando sea necesario ejercer el derecho a la libertad de expresión (para ello los países miembros tendrán que regular los límites de acuerdo con el principio de proporcionalidad); cuando sea necesario cumplir una obligación legal que se ampare en la Ley o se trate de interés público o ejercicio de poderes públicos conferidos al responsable (estamos hablando del poder de Estado frente al derecho de supresión/olvido); cuando se trate de razones de interés público en el ámbito de la salud pública, fines de archivo de interés público, investigación científica o histórica o fines estadísticos o cuando se trata de ejercicio de reclamaciones (formulación, ejercicio o defensa).

Vemos por tanto que priman las razones de interés público ante el derecho al olvido, un "nuevo" derecho comprendido en el marco digital e incorporado en el art.17 del reglamento. Existe un debate respecto de si el derecho al olvido es un derecho de nueva configuración o si por el contrario es un derecho mezcla derivado de los derechos

de acceso, rectificación, cancelación y oposición (en adelante los derechos ARCO)[48] y en cuanto a su alcance[49].

Señala REBOLLO DELGADO que con el derecho al olvido "se pretende el contenido protegido en el art.10.1 CE, dignidad de la persona y el libre desarrollo de su personalidad, que canalizado a través del art.18.1CE, pretende la salvaguarda del derecho al honor, la intimidad o la propia imagen".

No existe pues, un derecho al olvido absoluto y habrá que tener en cuenta la ponderación de intereses en juego[50].

---

[48] ARENAS RAMIRO, M. "Hacía un futuro derecho al olvido de ámbito europeo" en "La Protección de los Datos Personales en Internet ante la Innovación Tecnológica" Coordinador VALERO TORRIJOS J.,pp. 332-333, Ed.Thomson Reuters Aranzadi, Navarra, 2013.

[49] En las enmiendas al Reglamento, así como en las conclusiones presentadas por el Abogado General, alegaba que *"la Directiva no establece un derecho general al olvido, en el sentido de que un interesado esté facultado para restringir o poner fin a la difusión de datos personales que considera lesivos o contrarios a sus intereses. La finalidad del tratamiento y los intereses a los que sirve, al compararse con los del interesado, son los criterios que han de aplicarse cuando se procesan datos sin el consentimiento del interesado, y no las preferencias subjetivas de éste. Una preferencia subjetiva por sí sola no equivale a una razón legítima, en el sentido del art.14, letra a), de la Directiva" (108).*

[50] En este sentido se pronunció el TJUE en su Sentencia ASNEF y FECEMD, de 24 de noviembre de 2011 (asuntos C-468-10 y C-469-10); ***Sentencia*** Tribunal de Justicia de la Unión Europea (Gran Sala) Caso Google Spain S.L contra Agencia Española de Protección de Datos (AEPD). Sentencia de 13 mayo 2014. TJCE 2014\85 asunto C-131/12, considerando 81*:"Vista la gravedad potencial de esta injerencia, es obligado declarar que el mero interés económico del gestor de tal motor en este tratamiento no la justifica. Sin embargo, en la medida en que la supresión de vínculos de la lista de resultados podría, en función de la información de que se trate, tener repercusiones en el interés legítimo de los internautas potencialmente interesados en tener acceso a la información en cuestión, es preciso buscar, en situaciones como las del litigio principal, un justo equilibrio, en particular entre este interés y los derechos fundamentales de la persona afectada con arreglo a los artículos 7 y 8 de la Carta (LCEur 2000, 3480)* . ***Aunque, ciertamente, los derechos de esa persona protegidos por dichos artículos prevalecen igualmente, con carácter general, sobre el mencionado interés de los internautas****, no obstante* ***este equilibrio puede depender, en supuestos específicos, de la naturaleza de la información de que se trate y del carácter sensible para la vida privada de la persona afectada y del interés del público en disponer de esta información,*** *que puede variar, en particular, en función del papel que esta persona desempeñe en la vida pública."* – el cual culmina con la **Sentencia de 11 mayo 2017. RJCA 2017\487, de la Audiencia Nacional (sala de lo Contencioso-Administrativo) (FJ7).** *"Ya hemos dicho que conforme a los criterios de ponderación fijados en la sentencia del TJUE de 13 de mayo de 2014 el interesado 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, derechos que prevalecen, en principio, no sólo sobre el interés económico del gestor del motor de búsqueda, y sobre el interés de dicho público en acceder a la mencionada información en una búsqueda que verse sobre el nombre de esa persona. Mas también, siguiendo la misma doctrina del TJUE que tal criterio general resulta excepcionado si, por razones concretas, como el papel desempeñado por el interesado en la vida pública, 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. Doctrina general que asimismo se desarrolla en los apartados 81, 93 y 97 de la repetida sentencia del TJUE al indicar que, no obstante aquella*

4)derecho a la limitación de tratamiento: El interesado tiene derecho a limitar sus datos, es decir, que se limite el uso de los mismos sin proceder a la supresión. Ello será posible por ejemplo mientras el responsable verifica la exactitud de los datos (debido a la impugnación previa). Mientras dure el proceso de verificación el responsable procederá no a la supresión sino a la limitación. También se contempla esta posibilidad en el caso cuando el tratamiento no sea lícito, pero el interesado solicite solamente tal limitación; cuando se haya extinguido el fin con el que se trataban los datos, pero el interesado los necesite para el ejercicio de formulación, o defensa de una reclamación o cuando se haya ejercitado el derecho de oposición, pero está pendiente de verificar si el interés del responsable no prevalece sobre el interés de la persona que ejercita el derecho.

5) derecho a la portabilidad de datos: Se establece el derecho a que el interesado pueda recibir los datos personales que le incumban en un formato estructurado, de uso común y lectura mecánica en el caso en el cual el tratamiento se efectúe por medios automatizados. Se añade en el considerando 68 del RGPD la palabra interoperable, que viene a significar "la capacidad de los sistemas de información y de los procedimientos a los que éstos dan soporte, de compartir datos y posibilitar el intercambio de información y conocimiento entre ellos"[51]. Por tanto, **se motiva a los responsables que elaboren formatos que permitan compartir datos.** Asimismo, se establece una libertad de disposición de sus propios datos subrayando que el responsable que los facilite no puede impedir que el interesado los trasmita a otro responsable; sin embargo, ello es así solamente en los casos de un consentimiento expreso (se excluyen

---

prevalencia: hay que buscar un justo equilibrio entre el interés legítimo de los internautas en tener acceso a la información en una búsqueda que verse sobre el nombre de una persona y los derechos fundamentales de la misma y puede resultar que, por razones concretas, como el papel desempeñado por el mencionado interesado en la vida pública, 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". En 2017 se ha vuelto a plantear una cuestión prejudicial al TJUE respecto a la cuestión de retirada de los datos de los motores de búsqueda por parte de Commission nationale de l'informatique et des libertés (CNIL) contra Google INC http://curia.europa.eu/juris/document/document.jsf?mode=req&pageIndex=1&dir=&occ=first&part=1&text=protecci%25C3%25B3n%2Bde%2Bdatos&doclang=ES&cid=470972#ctx1 Consulta 3.02.2018

51 https://administracionelectronica.gob.es/pae_Home/pae_Estrategias/pae_Interoperabilidad_Inicio.html#.Wnny5ajiY2w Consulta 02.02.2018

excepciones que no están basadas en el consentimiento) o cuando se trate de un contrato. También podrán transferirse los datos de un responsable a otro.

En mi opinión, dicho precepto tiene su fundamentación en una facilidad de contratación en el marco de contrataciones electrónicas. Hoy en día al cambiar de un proveedor de servicios telemáticos es suficiente consentir la transferencia de nuestros datos de uno a otro para su formalización.

La motivación dirigida hacia los responsables a promover los formatos compatibles se hace, a mi entender, precisamente para eliminar las fronteras para la transferencia de datos entre los operadores, facilitando el tráfico económico y la circulación de datos, adoptando por supuesto las debidas garantías para ello. Asimismo, de esta manera se obliga a los operadores económicos a renovar sus sistemas *pro consumidor* (aunque ello pueda suponer grandes costes, toda vez que una renovación de sistemas no es nada trivial).

En cuanto al fichero estructurado, y para entender mejor el concepto, cuando hablamos de datos estructurados nos referimos a la información que se suele encontrar en la mayoría de bases de datos. Son archivos de tipo texto que se suelen mostrar en filas y columnas con títulos. Son datos que **pueden ser ordenados y procesados fácilmente por todas las herramientas de minería de datos. Lo podríamos ver como si fuese un archivador perfectamente organizado donde todo está identificado, etiquetado y es de fácil acceso[52]. Es decir,** que se trata de un formato que pueda ser procesado fácilmente por distintos programas o artilugios informáticos, o de otra manera que no sea incompatible con otros sistemas.

Añade el considerando 68 que no se pueden exigir tales formatos a la Administración Pública y, si se trata de grupos de personas el derecho a portabilidad, se tiene que entender sin perjuicio de otras personas.

6)derecho de oposición: se puede formular por parte del interesado en los casos previstos en el art. 6.1 e) y f) , es decir, en aquellos donde el tratamiento tiene un fin de interés público o se trate de ejercicio de un poder público, o cuando el tratamiento es

[52] https://smarterworkspaces.kyocera.es/blog/diferencia-datos-estructurados-no-estructurados/ Consulta 1.02.2018

necesario para la satisfacción de intereses legítimos perseguidos por el responsable o por un tercero siempre y cuando no prevalezcan los intereses y derechos fundamentales de interesado (sobre todo si es un niño).

7)derecho a no ser objeto de una decisión automatizada (art. 22 y considerando 71): La elaboración de los perfiles y tratamiento automatizado de datos suponen muchas veces que el individuo se vea desprotegido frente a la toma de decisiones basadas en este tipo de procesamientos. En este sentido la persona tiene derecho sobre todo a conocer que existe un tratamiento automatizado y que se están elaborando unos perfiles en cuanto a su personalidad (considerando 63 del Reglamento). Este principio obedece sobre todo a posibles efectos jurídicos que puedan aparecer y que deriven de una decisión automatizada (es decir, que no tenga intervención humana) en el seno de las operaciones realizadas en línea (como ejemplo el reglamento especifica la contratación vía red o la denegación de crédito en línea).

Sin embargo, como toda regla, está sujeta a unas excepciones. El legislador comunitario señala que dicho derecho no se aplicará cuando se trate de ejecución contractual o cuando dicha decisión automatizada esté prevista por la Ley (que además tiene que prever un procedimiento con todas las garantías velando por los derechos y libertades del interesado) o cuando medie un consentimiento explícito para ello (siempre y cuando el responsable establezca unas garantías de un mínimo de intervención humana que permita al interesado opinar o impugnar las decisiones automatizadas). Se excluyen por supuesto las categorías especiales de datos (datos sensibles).

Podemos concluir que los derechos que fueron denominados ARCO se han extendido debido a continuos avances tecnológicos. El legislador comunitario se ha preocupado por añadir derechos nuevos como las decisiones automatizadas (que avanzan sobre todo en el ámbito de robótica) o limitación del uso de datos y estableció un mínimo de intervención humana que es indispensable para la seguridad jurídica.

Por todo ello, el Reglamento tiende a mejorar el control sobre los datos de carácter personal.

10.El responsable o corresponsable de tratamiento y sus responsabilidades.

Aparte de las obligaciones ya mencionadas y sobre todo la obligación del deber de informar, el responsable o corresponsable (cuando son varios[53]) de tratamiento acarrea una responsabilidad o una debida diligencia. Esta diligencia se tiene que llevar a cabo **desde el diseño y por defecto,** es decir, que, se trata de diseño de unas técnicas que ponderan la situación de la gravedad, contexto, la categoría de datos tratados, así como la tecnología disponible. Una elaboración ex ante y que se va a aplicar durante el tratamiento, o como señala la AEPD que " en la práctica, supone tener en consideración la privacidad y el cumplimiento de las normativas de protección de datos **desde la fase inicial del proyecto (**de la misma manera que se tienen en consideración el resto de requisitos funcionales y no funcionales) con el objetivo de que el proyecto se diseñe e incluso ajuste y desarrolle teniendo en consideración dichos requerimientos, de tal manera que la privacidad se integre en las nuevas tecnologías y prácticas empresariales directamente, desde el principio, como un componente esencial de la protección de la privacidad"[54].

Para cumplir con lo estipulado **debe aplicar las medidas técnicas y organizativas que demuestren que el tratamiento que realiza es acorde con el Reglamento**. Esto incluye una revisión periódica de las mismas, aunque la norma no especifica la frecuencia, utilizando la expresión "cuando sea necesario". Se pueden incluir como tales (cuando sea proporcionado) las políticas de datos o las adhesiones a los códigos de conducta o mecanismos de certificación, seudonimización o minimización de datos.

Como el segundo punto y obligación, tiene que llevar un registro de actividades por escrito[55] de tratamientos efectuados bajo su responsabilidad y que tendrá que

[53] Art.26 del RGPD

[54] Código de Buenas Conductas de Protección de Datos pág.20 https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/2017/Guia_Big_Data_AEPD-ISMS_Forum.pdf Consulta 20 de enero 2018

[55]Art. 30.5 (sólo se refiere a empresas de más de 250 empleados a menos que éstas utilicen categorías especiales de datos, que no lo hagan de forma ocasional o realicen tratamiento de datos relativo a condenas o infracciones)

presentar ante la autoridad de control **cuando ésta lo solicite** (es decir que no estamos hablando de un depósito de obligado cumplimiento, pero sí de llevanza de un registro). Dicho registro tiene que contener al menos:

- Su nombre y datos de contacto (y el de corresponsable del encargado y del delegado de protección de datos, si procede – en adelante DPD)
- Los fines del tratamiento
- Categorías de datos personales y categorías de interesados
- Destinatarios a los que se comunicaron o vayan a comunicarse los datos
- Transferencias de datos y la documentación de garantías adecuadas
- Plazos para la supresión de diferentes categorías de datos
- (no obligado) descripción general de las medidas técnicas y organizativas de seguridad

Las mismas obligaciones las tendrá el encargado (mediante el cual puede delegar las obligaciones con una relación contractual donde se terminen los derechos y obligaciones de ambas partes y en todo caso el contenido tiene que obedecer al art. 28 RGPD), que actúe por cuenta del responsable añadiendo el hecho de que tiene que tener registro que indique los nombres o nombre del encargado y nombres y datos de los responsables por cuenta de quienes actúe.

La **tercera obligación que se le exige al responsable de tratamiento es la de garantizar el nivel adecuado de seguridad** adecuado al riesgo que se traduce en la seudonimización y el cifrado de datos, garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas de tratamiento, capacidad de resolver los incidentes, y un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas, así como las posibles consecuencias de la destrucción, pérdida o alteración de datos.

Como **cuarta obligación se establece el deber de notificar ante la autoridad de control las violaciones de seguridad** que se produzcan en el seno de su actividad. Para ello dispone de un plazo de 72 horas después de haber tenido constancia de ello. Se plantea aquí un problema de determinación del momento en el que se produjo la violación o determinación del momento en el que el responsable tiene el conocimiento

de tal violación. En todo caso, si sobrepasamos el plazo estipulado tendremos que adjuntar los motivos que justifiquen la dilación.

Dicha notificación tiene que contener como mínimo la descripción de la naturaleza de la violación de la seguridad, y las categorías de datos y número de afectados (cuando sea posible), el nombre y los datos del DPD, descripción de las consecuencias y de las medidas adoptadas o propuestas para poner el remedio, incluyendo medidas para mitigar los efectos negativos de la violación de seguridad.

El mismo deber se prevé para el encargado de tratamiento para ante el responsable de tratamiento, aunque sin estipulación del plazo máximo.

El deber de notificación conlleva el de documentación de todas las violaciones de seguridad junto con las medidas correctivas adoptadas, que puede ser exigido por la autoridad de control.

Como **quinta obligación** se establece el **deber de comunicar las violaciones de seguridad al propio interesado** y que puede ser exigido por la autoridad de control. Dicha comunicación será obligatoria en el caso en el que la misma conlleve un alto riesgo para los derechos y libertades del interesado, con el fin de que éste adopte las medidas oportunas para salvaguardar sus derechos e intereses y, sólo en el caso cuando el responsable no haya adoptado medidas que protejan eficazmente los datos (por ejemplo mediante cifrado) o cuando persista el riesgo de lesión. No se exige este deber cuando suponga un esfuerzo desproporcionado, donde se procederá a una comunicación pública[56].

En la sexta posición se sitúa el **deber de evaluar el impacto de las operaciones de tratamiento en la protección de datos personales,** que es exigible en los casos previstos en el art. 35.3 RGPD., a saber, en caso de elaboración de perfiles, tratamientos a gran escala de categorías especiales de datos o datos relativos a condenas e infracciones o, en caso de observación a gran escala de una zona de acceso público. A

[56] Art. 34 RGPD

este respecto la AGPD ha elaborado una Guía para la Evaluación del Impacto donde recomienda llevar a cabo la misma en los siguientes casos[57]:

– Cuando se enriquezca la información existente sobre las personas mediante la recogida de nuevas categorías de datos o se usen las existentes con nuevas finalidades o en formas que antes no se usaban, en particular, si los nuevos usos o finalidades son más intrusivos o inesperados para los afectados.

– Cuando se lleve a cabo un tratamiento significativo no incidental de datos de menores o dirigido especialmente a tratar datos de estos, en particular si tienen menos de catorce años.

– Cuando se vaya a llevar a cabo un tratamiento destinado a evaluar o predecir aspectos personales relevantes de los afectados, su comportamiento, su encuadramiento en perfiles determinados (para cualquier finalidad), encaminado a tomar medidas que produzcan efectos jurídicos que los atañen o los afectan significativamente y, en particular, cuando establezcan diferencias de trato o trato discriminatorio~~8~~ o que puedan afectar a su dignidad o su integridad personal.

– Cuando se traten grandes volúmenes de datos personales a través de tecnologías como la de datos masivos (Big data), internet de las cosas (Internet of Things) o el desarrollo y la construcción de ciudades inteligentes (smart cities).

– Cuando se vayan a utilizar tecnologías que se consideran especialmente invasivas de la privacidad como la videovigilancia a gran escala, la utilización de aeronaves no tripuladas (drones), la vigilancia electrónica, la minería de datos, la biometría, las técnicas genéticas, la geolocalización, o la utilización de etiquetas de radiofrecuencia o RFID10 (especialmente, si forman parte de la llamada internet de las cosas) o cualesquiera otras que puedan desarrollarse en el futuro.

[57] Páginas 13 y 14 de la Guía https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_EIPD.pdf consulta 3.12.2018

– Cuando el tratamiento afecte a un número elevado de personas o, alternativa o adicionalmente, se produzca la acumulación de gran cantidad de datos respecto de los interesados.

– Cuando se cedan o comuniquen los datos personales a terceros y, en particular, siempre que se pongan en marcha nuevas iniciativas que supongan compartir datos personales con terceros que antes no tenían acceso a ellos, ya sea entregándolos, recibiéndolos o poniéndolos en común de cualquier forma.

– Cuando se vayan a transferir los datos a países que no forman parte del Espacio Económico Europeo (EEE) y que no hayan sido objeto de una declaración de adecuación por parte de la Comisión Europea o de la Agencia Española de Protección de Datos.

– Cuando se vayan a utilizar formas de contactar con las personas afectadas que se podrían considerar especialmente intrusivas.

– Cuando se vayan a utilizar datos personales no disociados o no anonimizados de forma irreversible con fines estadísticos, históricos o de investigación científica.

– Cuando la recogida tenga como finalidad el tratamiento sistemático y masivo de datos especialmente protegidos

Además, habrá que tener en cuenta "la existencia de riesgos específicos de seguridad que puedan comprometer la confidencialidad, la integridad o la disponibilidad de los datos personales y, especialmente, si estas situaciones de riesgo se producen cuando los datos circulan o se accede a ellos a través de redes de telecomunicaciones".

En todo caso, si existen dudas en cuanto a la evaluación y el posible riesgo, el Reglamento establece un mecanismo de consulta a la autoridad de control, la cual tendrá que responder en un plazo de 8 semanas prorrogables por un mes más justificando la dilación.

Por tanto, vemos que se establece un mecanismo previo de la evaluación de los posibles riesgos, especialmente en los datos automatizados de manejo a gran escala que utilizan ciertas tecnologías que facilitan el manejo de la información. Se da una

protección reforzada en este sentido, estableciendo la posibilidad de regular dicha medida estableciendo su obligado cumplimiento o incluso establecer sujeción a una autorización previa de tratar determinadas categorías de datos realizando la evaluación previa del impacto[58].

11.Control del cumplimiento mediante sanciones y multas.

Toda infracción del Reglamento tiene que ir acompañada de un apercibimiento, sanción o multa y en su caso de la debida indemnización de daños y perjuicios. Para ello las autoridades de control garantizarán las debidas multas administrativas que han de ser efectivas, proporcionadas y disuasorias. Además, se tendrán en cuenta las circunstancias de cada caso, la naturaleza, la gravedad, intencionalidad, medidas tomadas para paliar daños y perjuicios, infracciones anteriores, categorías de datos afectados[59], la forma de conocimiento de la infracción, la adhesión a los códigos de conducta, así como cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso.

Las multas dependiendo del caso pueden ascender a 10.000000 euros o 20.000 000 euros como máximo dependiendo de qué infracciones se trate. Las cuantías más altas corresponden a infracciones de los principios básicos, incluidas las condiciones para el consentimiento, los derechos de los interesados, las transferencias de datos, obligaciones con arreglo del capítulo IX o incumplimiento de una resolución o limitación temporal o definitiva de tratamiento o suspensión de flujos de datos, infracciones de resoluciones de autoridad de control.

Se deja la vía abierta al establecimiento de diversas sanciones de otra índole aplicables a las infracciones del Reglamento.

[58] Art.36.5

[59] Lo que difícilmente se da en el caso de la reciente sanción al Facebook que asciende a 1,2 millones de dólares, debido a una facturación mucho más elevada de dicha empresa y debido a que las infracciones de principios generales, en concreto el deber de información, así como el tratamiento de datos sensibles deberían ser sancionadas de una manera más restrictiva. De todos modos, por el momento es un precedente.

Toda persona que haya sufrido daños y perjuicios materiales o inmateriales como consecuencia de la infracción de la norma tiene derecho a recibir del responsable o encargado de tratamiento la debida indemnización[60].

Por tanto, son los Estados los que tienen que establecer los procedimientos de tutela de derechos para hacer efectivo el cumplimiento de la norma en cuestión. El Reglamento prevé los márgenes para aplicar donde las leyes de los miembros de la unión podrán establecer los márgenes de su aplicabilidad.

IV.CONCLUSIONES

El desarrollo del derecho fundamental a la protección de datos es consecuencia necesaria del desarrollo de la sociedad de la información. La normativa, aunque a paso lento, va adaptándose a las realidades creadas por ser humano. Por el momento, la armonización europea persigue el objetivo común de eliminar las desigualdades generadas por la distinta aplicación de la normativa en cuanto al tratamiento de los datos y a su libre circulación (que ante todo dificulta el tráfico económico), así como en consonancia se están eliminando barreras relativas al comercio electrónico (estrategias para el mercado único digital).

Como hemos podido observar, se han necesitado muchos años para desarrollar la normativa que se adecue al derecho a la protección de datos debida su estrecha vinculación con la evolución tecnológica, así como para contemplarlo como un derecho fundamental, autónomo e independiente. Lo destacable en esta materia es que estamos contemplando un derecho desarrollado en el marco de la era digital, donde la sociedad de la información avanza a un ritmo muy rápido.

El Reglamento introduce novedades en cuanto a los principios y creación de figuras nuevas estableciendo mecanismos más eficaces. Es probable que en un futuro se introduzcan auditorías anuales (a modo de auditorías contables) de cumplimiento de la

[60] Art.82 RGPD

normativa sobre protección de datos, puesto que la no obligación de rendir cuentas ante una autoridad de control puede provocar serios problemas.

Por otro lado, y en mi humilde opinión, el *privacy by default and design* sólo será efectivo y se llevará a cabo cuando esté sujeto a un control obligado y efectivo por parte de autoridades de control.

La respuesta de las legislaciones en un panorama de industria tecnológica necesita buscar respuestas rápidas y eficaces y, sin duda, requerirá de una respuesta muy temprana en cuanto a los avances contemplados en la tecnología de inteligencia artificial. La capacidad robótica de manejar los datos a gran escala supondrá desde luego un nuevo reto para el legislador. Las tecnologías como biometría, machine learning, agentes virtuales, toma de decisiones automatizadas por parte de robots requerirá de un minucioso análisis y adecuación en cuanto al sistema de protección de datos personales donde el nuevo Reglamento requerirá de varias correcciones o bien de una normativa nueva o normativa complementaria.

V.BIBLIOGRAFÍA:

ÁLVAREZ HERNANDO,J. "PRACTICUM PROTECCIÓN DE DATOS 2018," ED. THOMSON REUTERS, Número de Edición: 1 Fecha de Edición: 21/09/2017

HERNÁNDEZ LÓPEZ J.M., "El Derecho a la Protección de Datos Personales en la Doctrina del Tribunal Constitucional". Cuadernos Aranzadi de Tribunal Constitucional nº31, Aranzadi Doctrina (edición impresa), Navarra, 2013

LACASTA L., SANMARTÍ E., VELASCO J., "Auditoría de la Protección de Datos". Ed.Bosch, 2ª edición adaptada al RLOPD, 2009

PIÑAR MAÑAS J.L, Director, "Reglamento General de Protección de Datos"" Hacía un nuevo modelo europeo de privacidad". Ed. Reus, Madrid 2016.

REBOLLO DELGADO L., SERRANO PÉREZ M.M., "Manual de Protección de Datos", Ed.Dykinson, 2ª edición, Madrid, 2017

VALERO TORRIJOS J., "La Protección de los Datos Personales en Internet ante la Innovación Tecnológica", "Riesgos, amenazas y respuestas desde la perspectiva jurídica". Ed. Thomson Reuters Aranzadi., Primera edición 2013. Navarra.

VI.SENTENCIAS:

<u>TRIBUNAL CONSTITUCIONAL:</u>

Sentencia de Tribunal Constitucional 254/1993 de 20 de julio

Sentencia de Tribunal Constitucional 292/2000 de 30 de noviembre

Sentencia de Tribunal Constitucional 96/2012 de 7 de mayo

Sentencia Tribunal Constitucional 39/2016 de 3 de marzo

TRIBUNAL EUROPEO DE DERECHOS HUMANOS:

Sentencia de 3 de abril de 2007 (TEDH 2001, 552) Caso P.G. y J.H. contra Reino Unido

Sentencia de 4 diciembre 2008. (TEDH 2008\104) Caso S. y Marper contra Reino

Sentencia de 17 de diciembre de 2009, Caso de Bouchacourt vs Francia

USentencia de 18 de septiembre de 2014 (TEDH 2014, 66) Caso Brunet contra Francia

nido.

Sentencia de 3 de diciembre de 2015, Caso OF SÕRO v. ESTONIA 22588/08

Sentencia de 28 de noviembre de 2017, Asunto 70838/13 Caso ANTOVIĆ AND MIRKOVIĆ v. MONTENEGRO

Sentencia de 5 de septiembre de 2017 Asunto 61496/08,

TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA

Sentencia de 7 de mayo de 2009, Rotterdam vs. Rijkeboer, Asunto C-553/07,

Sentencia de 24 de noviembre de 2011, ASNEF y FECEMD, (asuntos C-468-10 y C-469-10);

Sentencia de 13 de mayo de 2014, Caso Google Spain S.L contra Agencia Española de Protección de Datos (AEPD). asunto C-131/12,

Dictamen de 26 julio 2017. TJCE 2017\193

TRIBUNAL SUPREMO:

Sentencia de 5 abril 210/2016, (RJ 2016\1006)

RECURSOS WEB:

Cristina Cullell March, "El principio de neutralidad tecnológica y de servicios en la UE: la liberalización del espectro radioeléctrico" Artículo: Revista de Internet Dret y Política

http://curia.europa.eu/juris/document/document.jsf?mode=req&pageIndex=1&dir=&occ=first&part=1&text=protecci%25C3%25B3n%2Bde%2Bdatos&doclang=ES&cid=470972#ctx1

https://administracionelectronica.gob.es/pae_Home/pae_Estrategias/pae_Interoperabilidad_Inicio.html#.Wnny5ajiY2w

https://www.ieee.org/index.html

https://smarterworkspaces.kyocera.es/blog/diferencia-datos-estructurados-no-estructurados/

https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/2017/Guia_Big_Dhttps://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_EIPD.pdf

ata_AEPD-ISMS_Forum.pdf
http://curia.europa.eu/juris/document/document.jsf?text=protecci%25C3%25B3n%2Bde%2Bdatos&docid=198949&pageIndex=0&doclang=es&mode=req&dir=&occ=first&part=1&cid=470972#ctx1

http://hudoc.echr.coe.int/eng?i=001-177867

http://www.agpd.es/portalwebAGPD/canaldocumentacion/docu_grupo_trabajo/wp29/common/Versiones_ingles/20171013_wp250_enpdf.pdf

https://www.boe.es/doue/2016/207/L00001-00112.pdf

http://www.evolutionoftheweb.com/ ,
http://www.evolutionoftheweb.com/?hl=es#/growth/day

http://www.repozytorium.uni.wroc.pl/Content/52920/09_Jakub_Rzucidlo.pdf

http://www.congreso.es/public_oficiales/L12/CONG/BOCG/A/BOCG-12-A-13-1.PDF
http://www.lamoncloa.gob.es/consejodeministros/Paginas/enlaces/101117enlacedatos.aspx https://www.dsb.gv.at/datenschutz-grundverordnung

https://www.parlament.gv.at/PAKT/VHG/XXV/ME/ME_00322/fname_635512.pdf

https://www.gov.pl/cyfryzacja/nowe-prawo-ochrony-danych-osobowych

https://www.gov.pl/cyfryzacja/dokumenty27

http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/4298343https://www.datatilsynet.dk/english/the-act-on-processing-of-personal-data/read-the-act-on-processing-of-personal-data/compiled-version-of-the-act-on-processing-of-personal-data/