Trabajo Fin de Grado

EL IMPACTO DEL *BIG DATA* EN LA PROTECCIÓN DE DATOS PERSONALES

Análisis de los avances normativos en materia de protección de datos

Presentado por:

Mar Guevara Sanmateo

Tutor/a:

José Díaz Lafuente

Grado en Derecho

Curso académico 2017/18

LISTA DE ABREVIATURAS UTILIZADAS EN ESTE TRABAJO

AEPD	Agencia Española de Protección de Datos
AN	Audiencia Nacional
ARCO	Acceso, Rectificación, Cancelación y Oposición
Art.	Artículo
CE	Constitución Española
DPA	Data Protection Act
DPO	Data Protection Officer
EDPS	European Data Protection Supervisor
EE.UU.	Estados Unidos
EU	European Union
FECEMD	Federación Española de la Economía Digital, ahora adigital
GDPR	General Data Protection Regulation 2016/679, of 27 April
GPS	Global Positioning System
GT 29	Grupo de Trabajo del Artículo 29
ICO	Information Commissioner's Office
LO	Ley Orgánica
LOPD	Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal
LOTARD	Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal
LSSI	Ley de Servicios de la Sociedad de la Información
OSI	Oficina de Seguridad del Internauta
RGPD	Reglamento Europeo General de

	Protección de Datos 2016/679 de 27 de abril de 2016
RLOPD	Reglamento de desarrollo de la Ley Orgánica de Protección de Datos RD 1720/2007
SAN	Sentencia Audiencia Nacional
STC	Sentencia del Tribunal Constitucional
SSTC	Sentencias del Tribunal Constitucional
STJUE	Sentencia del Tribunal de Justicia de la Unión Europea
TC	Tribunal Constitucional
TIC	Tecnologías de la Información y la Comunicación
TJUE	Tribunal de Justicia de la Unión Europea
TS	Tribunal Supremo
UE	Unión Europea

ÍNDICE

1. INTRODUCCIÓN

Debido a la gran importancia que día a día van ganando las tecnologías del *big data* o macrodatos[1], hemos creído oportuno llevar a cabo este trabajo basándonos en esa importancia, la aplicación que tiene en nuestra vida cotidiana y cómo puede llegar a afectar a nuestro derecho a la protección de datos, privacidad e intimidad. La realización de este trabajo llega en un momento de renovación del marco legislativo de protección de datos, tanto a nivel europeo con el nuevo Reglamento General de Protección de Datos; como a nivel nacional con el Proyecto de Ley Orgánica de Protección de Datos. El nuevo RGPD representa un gran avance legislativo respecto a la anterior Directiva 95/46/CE, debido a que ésta se hizo en un momento en el que la tecnología no había mostrado todo su potencial, y no abarcaba todas las finalidades y aplicaciones que tienen ahora las nuevas tecnologías.

A medida que iremos conociendo el *big data*, entenderemos su gran aplicabilidad en diversos aspectos de nuestra vida, en el tratamiento de los datos personales, además del peligro que supone su divulgación y utilización de manera incorrecta. Por todo esto consideramos que es importante conocer todo lo que implica la divulgación de nuestros datos personales en la interacción con Internet y las tecnologías, así como los derechos que podemos ejercer para protegerlos.

En muchas ocasiones no somos conscientes de hasta dónde pueden llegar nuestros datos personales, pero la “magia” del *big data* permite hacer un gran análisis de todos los datos que se obtienen de Internet y ordenarlos de tal manera que las empresas puedan sacar partido de éstos y realizar perfiles para llevar a cabo su actividad comercial de una manera más personalizada y precisa.

Estructuraremos este trabajo describiendo en primer lugar el fenómeno de los macrodatos para poner en antecedentes de lo que es y, así, poder entender mejor el ámbito de este trabajo; además de ver las virtudes y desafíos que nos presenta la aplicación de los macrodatos en el mundo tan

1 Debido a que macrodatos es la alternativa en español a la voz inglesa *big data*, utilizaremos en este trabajo de forma indistinta estos dos conceptos.

interconectado en el que vivimos; ya que el *big data* puede ser un gran aliado para nosotros y a la vez el peor enemigo de nuestros datos personales debido al tratamiento que se haga de ellos.

En el tercer epígrafe analizaremos el marco legislativo en el que nos encontramos a nivel europeo y nacional en la protección de datos personales. Veremos como durante el camino a una regulación que pueda cubrir todos los avances tecnológicos, nos hemos encontrado en una situación en la que la tecnología ha ido muy por delante de la legislación que se encontraba vigente y algunos de los intentos de regular las invasiones a la privacidad y los datos personales han sido insuficientes. Ya lo predecía Terceiro cuando por aquel entonces, sugería el concepto de "autopistas de la información", al hablar de la gran cantidad de información que se encontraría en la Web, y la gran evolución que se produciría; siguiendo el pensamiento de que en ese camino a la evolución gradual se cometerían muchas equivocaciones.[2] Los países europeos han tendido a ser más conservadores en materia legislativa que los EE.UU., ya que han decidido mirar por una mayor protección de la privacidad, especialmente por los datos personales. Esto ha implicado que, en muchas ocasiones, la UE haya sido más efectiva.[3] Esta desigualdad que se ha producido durante mucho tiempo entre la legislación y el avance tecnológico parece haberse solucionado con la entrada en vigor del RGPD que desarrollaremos detalladamente en este epígrafe tercero.

Por último, aplicaremos esta legislación al *big data* y a los derechos y deberes que tienen tanto los responsables del tratamiento de datos como los titulares de éstos; además de ver el efecto que tienen las leyes mencionadas sobre conceptos clave en la interacción con Internet y las tecnologías de la información y la comunicación (TIC), como son el consentimiento, el derecho a la intimidad y la privacidad, los datos personales, la anonimización de los datos y la creación de perfiles.

---

2 TERCEIRO, José B.: *Socied@d digit@al. Del homo sapiens al homo digitalis*, Alianza editorial, Madrid, 1996, p. 31

3 DRUMMOND, Víctor y traducción de ESPÍN ALBA, Isabel: *Derecho de las nuevas tecnologías*, Editorial Reus, Madrid, 2004, p. 66.

2. ESTUDIO DEL *BIG DATA*

2.1. Definición del *big data*

En el mundo tan global en el que vivimos es importante conocer todos sus aspectos, las tecnologías que interfieren y cómo nos puede ayudar o perjudicar el "universo digital". Por eso hemos creído oportuno centrarnos en explicar la importancia que tiene el *big data* y qué supone para el Derecho y para las personas que utilizan las nuevas tecnologías a su alcance.

Desde el inicio de la evolución de las TIC se ha sentido la necesidad de recoger, guardar, procesar y clasificar la información, dando lugar al nacimiento de los macrodatos. De hecho, es la gran demanda de información y conocimiento lo que ha impulsado la demanda de las TIC, ya que éstas tienen la función de procesar y transportar esta información.[4] Si buscamos un significado unificado de macrodatos nos encontramos con miles de ideas que intentan explicar algo inmaterial que se ha creado y evolucionado en muy poco tiempo. El gran uso que se hace de las nuevas tecnologías (webs, aplicaciones, servicios, etc.), ha incrementado la cantidad de información que se almacena cada día. Entendemos entonces que el *big data* es el tratamiento de esos enormes conjuntos de datos que con los métodos tradicionales de almacenamiento, acceso y análisis son inviables.[5] Según otra definición de *big data* se hace referencia a la gran cantidad de datos disponibles, un masivo volumen de datos que pueden ser utilizados con diversos fines y se encuentran al alcance de las empresas, de los Estados e incluso de los particulares que tengan los conocimientos para acceder a ellos.

Cuando hablamos de macrodatos, también se hace referencia al conjunto de tecnologías cuyo objetivo es tratar esa gran cantidad de datos, empleando complejos algoritmos y estadísticas con diversas finalidades[6] y, en base a estos resultados, tomar decisiones. Nos encontramos entonces con un

4 TERCEIRO, José B. y MATÍAS, Gustavo: *Digitalismo: el nuevo horizonte sociocultural*, Grupo Santillana de Ediciones, Madrid, 2001, p. 157

5 "Big-Data-Concepto" http://www.gti.es/es-es/Nextwave/Paginas/BigData/big-data-concepto.aspx

6 GARRIGA DOMÍNGUEZ, Ana, *Nuevos retos para la protección de datos personales. En la Era del Big Data y de la computación ubicua*, Dykinson, S.L., Madrid, 2015, p.28

análisis masivo de datos, que más adelante veremos lo que nos supone en nuestros derechos y libertades, en un mundo más interconectado día a día; y es esta capacidad de las organizaciones para recolectar, almacenar y analizar grandes cantidades de información no estructurada con el fin de encontrar patrones y correlaciones y conclusiones útiles, lo que se conoce como macrodatos[7]. Aún así, para analizar todos estos datos, estructurarlos y clasificarlos, se necesitan de una serie de tecnologías y técnicas que se conocen como minería de datos. La minería de datos se sirve de la integración de algoritmos y automatización del proceso. Las tecnologías del *big data* hacen uso de la minería de datos para buscar correlaciones en los datos que se recogen y almacenan.[8]

En un mundo tan digitalizado como en el que nos encontramos, donde nuestra vida está prácticamente en la red, es importante que se conozcan todos los peligros que ello comporta y cómo podemos actuar en el caso de que veamos que se ha vulnerado alguno de nuestros derechos. Pero hay que tener en cuenta que somos nosotros mismos los que difundimos de manera activa grandes cantidades de información personal en línea a través de los distintos proveedores de servicios de plataforma, que actúan a la vez como facilitadores de flujos de datos.[9] Por lo que cada "click" que demos en Internet, cada web que visitemos, incluso cada "like", se puede transformar en conocimiento y se pueden crear perfiles en función de este conocimiento. Perfiles, que pondrán en peligro nuestra privacidad, la reputación y, con esto, la libertad del individuo y su dignidad.[10] Este rastro, es la llamada huella digital[11], algo que nos define. La huella digital constituye la materia prima principal de la era digital, donde los

7 TENE, Omer: *Reforming data protection in Europe and beyond: a critical assessment of the second wave of global privacy laws*, en A. RALLO y R. MAHAMUT (dir), *Hacia un nuevo derecho europeo de protección de datos*, ed. Tirant lo Blanch, Valencia, 2015, p.144

8 GIL, Elena, *Big data, privacidad y protección de datos*. Agencia Española de Protección de Datos, Agencia Estatal Boletín Oficial del Estado, Madrid, 2016. Accésit en el Premio de Investigación de 2015, se puede encontrar en: https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common, p. 99

9 TENE, Omer: *Reforming data protection in Europe and beyond: a critical assessment of the second wave of global privacy laws*, cit, p.144

10 RALLO, Artemi: *El derecho al olvido en Internet: Google versus España*, Editorial Centro de Estudios Políticos y Constitucionales, Madrid, 2014, p.28

11 La huella digital es toda la información nuestra que vamos dejando en la red a medida que interactuamos en la red, recopilada gracias, por ejemplo, a las cookies que favorecen que nuestro ordenador sea único. Es una combinación de valores de datos que permiten identificar a una persona.

datos se han convertido en la principal fuente de negocio.[12] Esto ha sido en gran parte al cambio que se ha hecho de la web 1.0 a la web 2.0, que implica una interacción entre los usuarios de la web, lo que permite un intercambio de información constante. Con todo esto, cabe decir que el 70% del universo digital es generado por nosotros mismos a través de esta interacción con los diferentes servicios de la red[13].

Todo esto nos puede llevar a pensar que se ha producido el cambio humano que ya predecía Terceiro, del *homo sapiens* al *homo digitalis*.[14]

Cuando hablamos de *big data*, es inevitable hablar del consentimiento. En muchas ocasiones, otorgamos el consentimiento antes de saber exactamente qué información se va a extraer de nosotros e incluso para qué se va a utilizar, pero bien es cierto, que las entidades que recogen estos datos, tampoco pueden llegar a imaginarse el potencial que va a tener la información recogida. Normalmente el *big data* reutiliza datos que fueron obtenidos para una primera finalidad, y les otorga una finalidad nueva.[15] "*A dondequiera que se accede en Internet, se deja un rastro digital, de manera que, al ser cada vez mayor el número de actividades de nuestro quehacer cotidiano que se realizan en línea, irá aumentando la información que sobre nuestras ocupaciones, gustos y preferencias quede registrada."*[16] A través de nuestro rastro digital se obtienen miles de datos que combinados permiten extraer diversos perfiles que informan acerca de lo que somos y hacemos.[17]

El *big data* se aplica en dos fases:

- La primera fase consiste en un proceso que toma nuestros datos, los inserta en los algoritmos y construye modelos que nos permite realizar

12 VALLS, Josep-Francesc: *BIG DATA: atrapando al consumidor*, Profit editorial, Barcelona, 2017, p. 41

13 CRAIG, Terence y LUDLOFF, Mary E.: *Privacy and Big Data,* O'Really, 2011, Sebastopol, chapter 1.

14 TERCEIRO, José B.: *Socied@d digit@al. Del homo sapiens al homo digitalis*, cit, p. 32

15 GIL, Elena, *Big data, privacidad y protección de datos, cit.*, p. 25

16 Recomendación 97/3, de 3 de diciembre de 1997, del Grupo de Trabajo del artículo 29 sobre el "*anonimato en Internet"*

17 CRAIG, Terence y LUDLOFF, Mary E.: *Privacy and Big Data, cit. chapter 1*

inferencias.[18] Es importante saber que los datos recopilados han sido asociados de manera correcta.

- La segunda fase es en la que el nuevo conocimiento se puede utilizar para tomar decisiones. Fase donde puede surgir un mayor riesgo para la privacidad de las personas.[19]

2.2. Ventajas del *big data*

Los macrodatos nos han permitido desarrollar campos hasta el momento desconocidos y han ayudado a explotar las tecnologías para el beneficio de nuestra economía. Un gran beneficio de los macrodatos hoy en día es su utilización para poder realizar una publicidad más personalizada y poder llegar a un mayor número de personas interesadas en lo que se ofrece. Los macrodatos nos permite poder prever también fluctuaciones en el comportamiento de la gente y poder estar preparado para cualquier imprevisto que surja, como por ejemplo, un mercado, que gracias a la aplicación del *big data*, sabe cuándo y de qué productos proveerse más.

La digitalización, la globalización y la conectividad rompen las viejas estructuras y permiten abordar al consumidor de una manera distinta, presentándole una oferta que aporte más valor.[20]

Las grandes empresas supieron ver el valor potencial de las técnicas del *big data* y la minería de datos hace años, y así Axciom[21], Google, IBM (*International Bussiness Machines Corporation*) o Facebook llevan años invirtiendo en descubrir nuevos usos de los datos, cómo tratarlos y cómo transformarlos en valor. Este nuevo conocimiento, permite a las empresas crear nuevos servicios y productos más adaptados a las necesidades de las personas, lo que les permite tener una gran ventaja competitiva.[22]

---

18 Inferencia es que es la posibilidad de deducir, con probabilidad significativa, el valor de un atributo de los valores de un conjunto de otros atributos, según el GRUPO DE TRABAJO DEL ARTÍCULO 29. «Opinion 05/2014 on Anonymisation techniques» (2014).

19 GIL, Elena, *Big data, privacidad y protección de datos, cit. pp.55 y ss.*

20 VALLS, Josep-Francesc: *BIG DATA: atrapando al consumidor*, cit., p. 143

21 Acxiom proporciona los datos, la tecnología y los servicios que se necesitan para impulsar las experiencias excepcionales de los clientes en cualquier lugar, es decir, lleva a cabo análisis de *big data* para las empresas. Se puede encontrar en Acxiom: *https://www.acxiom.com/what-we-do/*

22 GIL, Elena, *Big data, privacidad y protección de datos, cit. p.29*

Los consumidores cada vez son más exigentes y los datos seleccionados e integrados y las analíticas proporcionadas por los macrodatos, permiten que se tenga un conocimiento suficiente de los clientes para poder adelantarse a sus necesidades y aspiraciones, que faculta que las empresas actúen en tiempo real y, así, poder fidelizar a los clientes con mayor facilidad.[23]

Con el avance del *big data* nos encontramos con la creación de la publicidad conductual o publicidad dirigida (*Behavioral adversiting*), que es una forma de predecir, mediante el comportamiento de los usuarios, qué servicio o producto podría interesarte comprar. Nos encontramos agrupados en términos de nuestro comportamiento y estos grupos se alquilan o se venden a anunciantes que desean vendernos algo.[24] Con esto, las empresas pueden llegar a un público más interesado en sus anuncios, lo que significa vender más. Otro aspecto es el "marketing de ubicación"[25], en el que se ofrecen avisos basados en su ubicación (GPS del móvil), como ocurre con los consejos de Google sobre hacer fotos o valorar un sitio en el que te encuentras.

Otro aspecto de la publicidad que se ha visto beneficiada es la publicidad en línea. Mientras navegamos en Internet podemos ver publicidad en cada página web que es modificada según los datos que Internet obtiene de nosotros, según las búsquedas realizadas y los datos que vamos introduciendo. Desde la perspectiva de la empresa publicitaria, Internet es único en cuanto a la cantidad de información que puede generar y recopilar sobre individuos y grupos de personas, lo que lleva a una mayor calidad y a una segmentación más específica. Desde la perspectiva de la página donde aparece la publicidad, la publicidad en línea es un gran negocio, ya que cobran de las empresas para que se publiciten en sus páginas, y hoy en día casi cualquier sitio puede incorporar publicidad en su modelo de negocio como un canal de ingresos.[26]

23 VALLS, Josep-Francesc: *BIG DATA: atrapando al consumidor*, cit., p.10.
24 CRAIG, Terence y LUDLOFF, Mary E.: *Privacy and Big Data, cit. chapter 1*
25 CRAIG, Terence y LUDLOFF, Mary E.: *Privacy and Big Data, cit. chapter 1*
26 CRAIG, Terence y LUDLOFF, Mary E.: *Privacy and Big Data, cit. chapter 4*

Terceiro ya apreciaba que el comercio no volvería a ser el mismo debido al comercio interactivo afectando a la publicidad con los “interanuncios”, diseñados para un tipo específico de consumidor.[27]

De los macrodatos no solo se pueden beneficiar las empresas, sino también las Administraciones Públicas, el sector sanitario y el sector financiero y bancario. El uso de los macrodatos puede implicar una toma de decisiones más rápida y eficaz, poder realizar análisis predictivos o una mejora continua de los sistemas de trabajo, además de mejorar la eficiencia.[28]

Los macrodatos también nos ofrecen una comunicación instantánea y una navegación más completa por la red, gracias a la gran información que retienen los buscadores sobre nuestras preferencias.[29]

2.3. Inconvenientes del *big data*

“Lo que está en juego nunca ha sido tan alto”[30]. Debido a la gran cantidad de interacciones diarias en la red y debido al uso que de la información intercambiada realizan las compañías y los Estados, nos encontramos con nuevos retos en el ámbito de la infracción a los derechos fundamentales.[31] Como era de prever, no todos son ventajas en la implantación del uso del *big data*. Principalmente hay tres aspectos en los que puede ser negativa la aplicación del *big data*. Estos son: 1. el riesgo de incurrir en conclusiones erróneas que una persona no revise, ya que estamos expuestos a encontrar relaciones entre información que no tienen ningún tipo de relación que puede ser debido a la casualidad o al puro azar. 2. El riesgo que para las personas pueda tener tomar decisiones automatizadas sin una supervisión humana, ya que confiar ciegamente en los algoritmos lleva a que en muchas ocasiones las empresas tomen decisiones sobre nosotros sin que podamos saber por qué las han tomado[32], como por ejemplo, cuando acudimos a una tienda para realizar una compra a plazos, se realiza un estudio que se basa en

27 TERCEIRO, José B.: *Socied@d digit@al. Del homo sapiens al homo digitalis*, cit., p.133
28 GIL, Elena, *Big data, privacidad y protección de datos, cit. p. 30*
29 CRAIG, Terence y LUDLOFF, Mary E.: *Privacy and Big Data, cit. chapter 1*
30 CRAIG, Terence y LUDLOFF, Mary E.: *Privacy and Big Data, cit. chapter 1*
31 GARRIGA DOMÍNGUEZ, Ana, *Nuevos retos para la protección de datos personales. En la Era del Big Data y de la computación ubicua*, cit. p. 25
32 GIL, Elena, *Big data, privacidad y protección de datos, cit. p. 42*

introducir nuestros datos en un programa y éste decide, en base a unas puntuaciones y a la revisión de unas bases de datos, si nos conceden o no ese crédito. Todo esto, gracias al uso de nuestros perfiles que puede llegar a encuadrar la información a la que tenemos acceso, puede determinar la toma de decisiones en diferentes aspectos de nuestra vida cotidiana y determinar, de algún modo, la personalidad de las personas.[33] Como indica la autora Álvarez, en la era del Internet de las cosas, en todo momento generamos información de nuestra interacción con la red relacionada con nuestra vida que, combinada y segmentada de acuerdo con determinadas correlaciones más o menos afortunadas pueden predeterminar que una persona, pueda acceder o no, a un determinado tipo de producto o servicio[34]. Veremos más adelante como el nuevo Reglamento de Protección de Datos ha tenido en cuenta este aspecto. Y 3. el riesgo para la privacidad de las personas y la volación de los datos personales.[35] El empleo de los macrodatos implica en muchas ocasiones una intrusión en nuestro derecho fundamental a la protección de datos personales que deriva directamente de la Constitución y que se encuentra regulado en la Ley Orgánica 15/1999, de Protección de Datos Personales (LOPD); además de una seria intrusión en nuestro derecho a la privacidad. Con la expansión de Internet, se ha ampliado la amenaza al derecho a estos derechos, ya que a través de las *cookies*[36] o programas de rastreo, se posibilita el funcionamiento de las denominadas "redes de seguimiento".[37]

En la actualidad, la cadena de emisores y receptores de datos es potencialmente infinita, e incluye actores e instituciones cuyo rol y

33 GARRIGA DOMÍNGUEZ, Ana, *Nuevos retos para la protección de datos personales. En la Era del Big Data y de la computación ubicua*, cit. p. 69

34 ÁLVAREZ, Cecilia: *El poder del usuario digital*, en A. RALLO y R. MAHAMUT (dir), cit, p.305

35 GIL, Elena, *Big data, privacidad y protección de datos, cit. p. 32*

36 Las cookies son fragmentos de programa necesarios para desarrollar muchas de las acciones que ejecutamos en Internet. Estos archivos de texto, a menudo encriptados, se ubican en el navegador de cada usuario, de manera que el sitio Web puede consultar la actividad previa de éste y sus preferencias. En NOAIN SÁNCHEZ, Amaya: *La protección de la intimidad y vida privada en Internet: la integridad contextual y los flujos de información en las redes sociales (2004-2014)*, Agencia Española de Protección de Datos, Agencia Estatal Boletín Oficial del estado, Premio Protección de Datos Personales de Investigación 2015. Madrid, 2016, podemos encontrarlo en https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/premios_2015/La_proteccion_de_la_intimidad.pdf, p. 312

37 GARRIGA DOMÍNGUEZ, Ana, *Nuevos retos para la protección de datos personales. En la Era del Big Data y de la computación ubicua*, cit. p. 23

responsabilidades no están delimitados o comprendidos[38], por lo que puede poner en grave peligro nuestros derechos fundamentales citados anteriormente y aún más complicado puede resultar el controlarlo. En muchas ocasiones, se considera que la anonimización supone una ayuda en la protección de los datos personales, sin embargo la reidentificación, supone otro riesgo para la privacidad de las personas (en el apartado 3, entraremos a explicar mejor estos métodos). Terceiro ya advertía del problema actual de la gran cantidad de información que tienen las empresas, que supone un riesgo de manipulación y su utilización posterior.[39]

Pero no solo los macrodatos ponen en peligro nuestros derechos de protección de datos y privacidad, sino la introducción en nuestra vida diaria de lo denominado Internet de las cosas (*Internet of Things*), donde encontramos objetos que monitorizan nuestro día a día, como son los controladores inteligentes, los dispositivos de geolocalización, etiquetas RFID[40] y la tecnología del monitoreo[41]; todas éstas se van viendo mejoradas y superadas por otras y por las diferentes aplicaciones que se hacen de estas tecnologías.[42]

La tarea de garantizar la seguridad de los datos y la protección de la privacidad se debe llevar a cabo por las entidades que recaban estos datos y de controlar que esto se cumpla, deben hacerse cargo diferentes entidades creadas ex profeso para ello. En este ámbito, podemos encontrar a la Agencia Española de Protección de Datos (AEPD), para hacer cumplir toda la normativa vigente y promover el desarrollo de normativas y guías a seguir tanto por consumidores, como por empresas; también nos encontramos con el Grupo de Trabajo del 29, mencionado anteriormente, que, aunque sus informes no son de obligado cumplimiento, sí que sirven de base para poder establecer unas bases de “buen comportamiento” en Internet. Otra entidad que ayuda a controlar que se respeten los derechos de los usuarios es la Oficina de

38 GIL, Elena, *Big data, privacidad y protección de datos, cit. p. 73*

39 TERCEIRO, José B.: *Socied@d digit@al. Del homo sapiens al homo digitalis*, cit., p.134.

40 Se trata de una tecnología diseñada para identificar y localizar objetos de forma automática gracias a una onda emisora incorporada en el dispositivo, “que transmite por radiofrecuencia los datos identificativos del objeto, siendo esta identificación normalmente unívoa” Guía sobre seguridad y privacidad de la tecnología RFID, de Inteco y la Agencia Española de Protección de Datos, 2010.

41 CRAIG, Terence y LUDLOFF, Mary E.: *Privacy and Big Data, cit. chapter 1*

42 GARRIGA DOMÍNGUEZ, Ana, *Nuevos retos para la protección de datos personales. En la Era del Big Data y de la computación ubicua*, cit. pp. 25 y ss

Seguridad del Internauta[43] (OSI), que proporcionan la información y el soporte necesarios para evitar y resolver los problemas de seguridad que pueden existir al navegar por Internet.

Lo que para las empresas, hemos visto que es una ventaja (publicidad específica), resulta una intrusión para nosotros. Las empresas rastrean nuestro comportamiento, principalmente a través de las *cookies* que permiten, a sabiendas o no, instalarse en tu escritorio o dispositivo para recopilar información y luego poder utilizarla o venderla.[44] Por lo que, muchas veces, cuando damos información a una página para acceder a contenido gratuito, nos acaba costando nuestra privacidad.

De todo esto, se benefician los proveedores de datos o mercados de datos, que son los intermediarios, como InfoChimps, Gnip, Neilsen, Rapleaf, etc[45]. Éstos operan como intermediarios, realizan análisis y otros servicios para ayudar a transformar los datos en información sobre la que se puede actuar. Si bien los mercados pueden estar sujetos a políticas de privacidad ubicuas de los recolectores y tienen sus propias políticas de privacidad, no está claro cómo el uso de datos puede controlarse y hacerse cumplir una vez que los datos cambian de manos tantas veces.[46]

43 OSI: https://www.osi.es/es
44 CRAIG, Terence y LUDLOFF, Mary E.: *Privacy and Big Data, cit. chapter 1*
45 Diferentes empresas dedicadas al tratamiento del big data y que ofrecen sus servicios a otras empresas que necesiten la información ya convertida en conocimiento.
46 CRAIG, Terence y LUDLOFF, Mary E.: *Privacy and Big Data, cit. chapter 4*

3. ANÁLISIS DEL MARCO NORMATIVO EN PROTECCIÓN DE DATOS Y PRIVACIDAD

En este epígrafe nos centraremos en la legislación general que se debe conocer a la hora de hablar de protección de datos y privacidad. Existen otros tipos de leyes más concretas según el ámbito tecnológico, pero haremos referencia a alguna de las leyes generales y que constituyen la base de este ámbito. En este trabajo nos limitaremos a las leyes españolas y comunitarias que son de aplicación en nuestro territorio.

A pesar de que Internet es global, la privacidad no lo es, por lo que las leyes de privacidad y las medidas y organismos reguladores difieren de un país a otro[47]. Esto es así, debido a que, por ejemplo, en Europa, cada país introduce las Directivas de una manera concreta y con algunas diferencias. Y aún más desigualdad encontramos con países no pertenecientes a la Unión Europea, donde la percepción de privacidad y vida privada también cambia, por lo que el enfoque legislativo también es distinto; como por ejemplo en EE.UU., donde, en muchas ocasiones, en el debate entre seguridad y privacidad, la seguridad nacional se encuentra por encima, y más, a raíz del atentado del 11-S.

En una charla en el *Personal Democracy Forum* 2011, Danah Boyd postuló que, dado a que nuestros datos e interacciones están conectados, nuestra privacidad también está conectada. *"Nuestras leyes se centran en la recopilación de datos, no en el uso de datos. Y, sin embargo, es en el nivel de uso donde se producen las violaciones de la privacidad..."*.[48]

Las leyes de protección de datos están diseñadas para proteger nuestra información personal tanto en línea como sin conexión; sin embargo, las leyes de retención de datos determinan cuánto tiempo los datos, incluido los personales, deben ser retenidos por una entidad para fines legales o comerciales. Ambos aspectos pueden tener un impacto en la privacidad de las comunicaciones, el comportamiento y la persona en diferentes maneras.[49] Esto es debido a que no solo se retiene esa información, sino que ésta puede ser

47 CRAIG, Terence y LUDLOFF, Mary E.: *Privacy and Big Data, cit. chapter 1*
48 CRAIG, Terence y LUDLOFF, Mary E.: *Privacy and Big Data,* cit. chapter 2
49 CRAIG, Terence y LUDLOFF, Mary E.: *Privacy and Big Data,* cit. chapter 2

utilizada para fines muy distintos de los que no tenemos conocimiento, algunos de estos fines los hemos podido ver en el anterior epígrafe.

Según Terence Craig y Mary E. Ludloff, Europa ha adoptado el modelo regulatorio de leyes integrales, en el que las leyes generales rigen la recopilación y el uso de información personal por parte de los sectores públicos y privados y estas leyes suelen ir acompañadas de un órgano de supervisión para garantizar su cumplimiento[50], como es el caso en España de la AEPD, que se encarga de que la legislación sobre la protección de datos se aplique de una manera correcta y de llevar a cabo las acciones correspondientes para resarcir los derechos de los perjudicados.

Conforme a lo que dice José Miguel Hernández, las leyes actuales son las que se consideran las leyes de tercera generación y que buscan el equilibrio entre la protección de datos personales (concepto que veremos con detalle en el apartado 4º de este trabajo) y el derecho a la información, además de dar respuesta a los riesgos que la tecnología nos presenta y su incidencia en los derechos fundamentales, como es el caso de la Directiva 95/46/CE.[51]

3.1. Normativa europea

3.1.1. Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos

En el ámbito europeo nos encontramos con la Directiva 95/46/CE adoptada por el Parlamento Europeo y el Consejo de la Unión Europea (en adelante Directiva 95/46). Esta Directiva constituía (hasta el pasado 25 de mayo de 2018 que entró en vigor el nuevo RGPD) el texto de referencia en materia de protección de datos personales y creaba un marco regulador destinado a establecer un equilibrio entre un nivel elevado de protección de la vida privada de las personas y la libre circulación de datos personales dentro de la UE.[52] Fue adoptado con un doble objetivo: defender el derecho

50 CRAIG, Terence y LUDLOFF, Mary E.: *Privacy and Big Data,* cit. Chapter 3

51 HERNÁNDEZ LÓPEZ, José Miguel: *El Derecho a la Protección de Datos Personales en la Doctrinal del Tribunal Constitucional*, Thomson-Reuters Aranzadi, Navarra, 2013, p. 26

52 EUR-Lex, El acceso al Derecho de la Unión Europea: *https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=LEGISSUM%3Al14012*

fundamental a la protección de datos y garantizar la libre circulación de estos datos entre los Estados miembros. Esta Directiva se complementó mediante la Decisión Marco 2008/977/JAI del Consejo, de 27 de noviembre de 2008, relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal.[53]

Debido a que esta Directiva ya no se encuentra en vigor, haremos una breve referencia a las principales aportaciones de esta norma para poder centrarnos en la normativa vigente. La Directiva determina límites estrictos para la recogida y utilización de los datos personales y solicita la creación de un organismo nacional independiente encargado de la supervisión de cualquier actividad relacionada con el tratamiento de los datos personales[54] y así llevar la protección de éstos a través de la vía administrativa[55], como es el caso de España con la AEPD, que se encarga de velar por el cumplimiento de la legislación sobre la protección de datos y controlar su aplicación, en especial de los derechos de información, acceso, rectificación, oposición y cancelación de datos (los derechos ARCO).[56] El ámbito de aplicación de esta Directiva era el tratamiento de datos personales, ya sea de manera automatizada o no, cuando estaban destinados a incluirse en un fichero, así como la protección de los datos de especial protección, se incluyeron esta categoría de datos que son más sensibles para la identificación de las personas (art. 8) y siempre con la debida notificación al propietario de esos datos y notificación a la autoridad de control antes de su tratamiento.

Como se indica en su considerando 4, la Directiva intenta abordar el gran avance de las tecnologías de la información que facilitan tanto el intercambio de datos personales, algo que está haciendo que la privacidad se vea cada vez más mermada. Con esta Directiva se intenta que en todos los Estados miembros, se adopten medidas similares en cuanto al tratamiento y circulación de los datos para que haya una unanimidad en los derechos de

53 HERNÁNDEZ LÓPEZ, José Miguel: *El Derecho a la Protección de Datos Personales en la Doctrinal del Tribunal Constitucional*, cit., p. 37

54 GIL, Elena, *Big data, privacidad y protección de datos,* cit., p. 138

55 DRUMMOND, Víctor y traducción de ESPÍN ALBA, Isabel: *Derecho de las nuevas tecnologías*, cit., pp.69 a 72.

56 AGPD: *http://www.agpd.es/portalwebAGPD/LaAgencia/informacion_institucional/conoce/funciones-ides-idphp.php*

todos los ciudadanos europeos, sin embargo, como hemos indicado antes, cada Estado miembro aplica la Directiva de diferente manera, como se deduce de su considerando 9.

La Directiva incluyó un listado de definiciones que permitía poder tener una visión clara del avance informático y de su aplicación en la norma. La Directiva 96/46 intentó aclarar las reglas de aplicabilidad territorial en su art. 4.1.a) y en su Considerando 20[57], sin tener mucho éxito debido a los avances en el mundo tecnológico que se produjo posteriormente y a que se hizo a través de un lenguaje un tanto farragoso. Este problema lo hemos podido ver a lo largo de estos años con la gran cantidad de empresas, como Google, Facebook o Microsoft, que tienen sus sedes en un determinado país, pero tienen diferentes filiales y proporcionan servicio en multitud de países.

Otro gran avance de esta Directiva 95/46 es la introducción de los términos de supresión, rectificación y oposición del tratamiento de los datos personales cuando los titulares de éstos lo solicitaran. Como vemos en el art. 15, no se prohíbe expresamente la creación de perfiles, sino que se establecen unos límites para que los perfiles no sean creados de forma automatizada y sin intervención humana. La elaboración de perfiles permite que los individuos sean categorizados sobre la base de algunas características observables para así poder inferir otras que no lo son[58]; esto puede llevar a muchas equivocaciones si no se llegan a revisar los resultados de estas decisiones. Importante mención merece la referencia a la transferencia de datos personales a terceros países, ya que ha sido y sigue siendo un tema muy conflictivo. Esta referencia tiene como destinatario principal EEUU, ya que es un país que ofrece un grado de protección mucho menos que la UE, y cuyo número de empresas presentes en el mercado europeo es cada vez mayor.[59]

La creación por la Directiva 95/46 del Grupo Europeo de Protección de

57 Este Considerando intenta evitar que "*el hecho de que el responsable del tratamiento de datos esté establecido en un país tercero no debe obstaculizar la* protección de las personas" y que debe regir "*la legislación del Estado miembro en el que se ubiquen los medios utilizados"*.

58 GIL, Elena, *Big data, privacidad y protección de datos,* cit., pp. 124 y 128

59 DRUMMOND, Víctor y traducción de ESPÍN ALBA, Isabel: *Derecho de las nuevas tecnologías*, cit., p. 58

Datos del Artículo 29 (GT 29)[60] es un aspecto muy importante debido a su gran cantidad de directrices y dictámenes que han ayudado a la aplicación de la normativa a los grandes avances tecnológicos.

Los problemas que podemos encontrar en esta normativa europea son la falta de claridad en la definición de datos personales y del responsable del tratamiento de éstos, falta de transparencia en el deber de información, no existe uniformidad en determinados aspectos a la hora de aplicar la normativa de protección de datos, por ejemplo entre países europeos; poca flexibilidad cuando se intenta aplicar alguna categoría nueva o principios en materia de protección de datos personales y en la normativa que la envuelve; y el papel de las autoridades nacionales encargadas de la protección de datos es débil y no existe colaboración entre éstas.[61]

Que Internet sea tan global implica muchos peligros a la hora de establecer una legislación en concreto en el caso de las grandes empresas que tienen sedes en diferentes países, europeos o no. Este es el caso por ejemplo de Google Inc., donde se crea un problema a la hora de intentar buscar responsables de las violaciones en protección de datos personales ya que tiene su sede fuera de la UE: Google Inc.[62], por lo que cualquier controversia referida a las búsquedas se sometería exclusivamente a la legislación de EE.UU. Se considera que Google Spain es una mera empresa filial de Google Inc., cuyo objeto social es promover, promocionar y comercializar servicios de publicidad online mediante Internet[63]; por lo que no dispone de capacidad jurídica para prestar servicios del buscador. En este aspecto consideramos importante hacer referencia al Auto de 27 de febrero 2012,[64] en el que la Audiencia Nacional

60 Órgano independiente y que sus dictámenes tendrán unicamente carácter consultivo, el Grupo se encuentra integrado por las Autoridades de Protección de Datos de todos los Estados miembros, el Supervisor Europeo de Protección de Datos y la Comisión Europea.Podemos ver información del GT 29: *http://www.agpd.es/portalwebAGPD/internacional/Europa/grupo_29_europeo/index-ides-idphp.php*

61 ARENAS, Mónica: R*eforzando el ejercicio del derecho a la protección de datos personales: viejas y nuevas facultades*, en A. RALLO y R. MAHAMUT (dir), cit, pp. 316 a 319.

62 Empresa con sede en Mountain View, California; Google: *https://es.wikipedia.org/wiki/Google*

63 Objeto social de Google Spain: *http://empresite.eleconomista.es/GOOGLE-SPAIN.html*

64 RJCA 2012/321

plantea una cuestión prejudicial al Tribunal de Justicia de la Unión Europea.[65] El mayor problema que se plantea en esta sentencia es establecer si se aplicaría la Directiva 95/46 para tutelar el derecho a la protección de datos de un nacional español frente a la empresa Google Inc. y su filial Google Spain[66]; por lo que Google alega que el proceso del buscador no se realiza mediante medios que se sitúen en España, por lo que no tendría que estar sujeto a la legislación europea[67].[68] Por lo que al final entiende que en este caso es de aplicación la Directiva 95/46[69].[70] Actualmente existe una gran jurisprudencia en las que la AEPD reclama a Google el borrado de cierta información de su buscador que solicitan distintos ciudadanos y en la gran mayoría, ya se hace referencia al derecho al olvido. Sin embargo, el caso de referencia en el que el

65 En este asunto un individuo se pone en contacto con Google Spain S.L. para que borre unos links, ejerciendo su derecho de oposición, a La Vanguardia (que previamente ésta había rechazado aceptar) que aparecen cuando se realiza la búsqueda de su nombre en el buscador sobre una subasta que ya ha sido resuelta; Google Spain remite a que se ponga en contacto con Google Inc., por lo que esta persona solicita ayuda a la AEPD. La AEPD inició un expediente administrativo por denegación del derecho de cancelación de los datos y finalmente estimó la reclamación y solicitó a Google Spain y Google Inc, que retirara los datos; pero posteriormente estas empresas recurrieron por separado.

66 En este aspecto, se deberán de tener en cuenta el considerando 19 y 20 de la Directiva 95/46, pero al no ser del todo claros los términos en los que se redactan estos textos, es el Tribunal quien tiene que considerar si entraría en estos supuestos.

67 En varios puntos de esta sentencia se hace referencia al Dictamen 1/2008 sobre motores de búsqueda en Internet, de 4 de abril de 2008, del Grupo de Trabajo del art. 29, donde se limita la responsabilidad de los buscadores, en cuanto responsables del tratamiento, únicamente a determinadas obligaciones de la Directiva 95/46.

68 Consideramos importante reseñar este punto de la sentencia, debido a que muestra un aspecto al que hacemos referencia en varios puntos en este trabajo: "*Internet traspasa fronteras y límites temporales y los buscadores potencian ese efecto, permitiendo una difusión global de esa información y facilitando su localización*. *[…] Las herramientas tecnológicas actuales, especialmente los motores de búsqueda, potencian que los afectados estén sometidos permanentemente a la exposición pública y general […].*" en la contestación a la cuestión prejudicial. Sentencia 13 de mayo de 2014 del TJUE.

69 Indica que es de aplicación la Directiva 95/46 al considerar "*que el tratamiento de datos personales realizado en orden al funcionamiento de un motor de búsqueda como Google Search, gestionado por una empresa que tiene su domicilio social en un Estado tercero pero que dispone de un establecimiento en un Estado Miembro, se efectúa en el marco de las actividades de dicho establecimiento si éste está destinado a la promoción y venta en dicho Estado miembro de los espacios publicitarios del motor de búsqueda, que sirven para rentabilizar el servicio propuesto por el motor".*

70 Y finalmente en la SAN de 29 de diciembre de 2014 (RJCA 2014/1065), se indica que procede la desestimación del recurso contencioso-administrativo, por lo que se establece la obligación de adoptar las medidas necesarias para retirar o eliminar de la lista de resultados los vínculos a las páginas web objeto de reclamación. Posteriormente Google Spain interpone recurso de casación, ya que considera que no existe corresponsabilidad y finalmente en Sentencia 1611/2016 de 4 de julio del Tribunal Supremo se estima el recurso contencioso-administrativo, pero lo mantiene en cuanto a Google Inc. Vemos como ya en esta Sentencia se hace referencia al nuevo derecho al olvido que se introducirá con el Nuevo Reglamento de Protección de Datos.

TJUE confirmó la plena aplicabilidad de la Directiva de protección de datos a Internet, es el caso Lindqvist.[71]

Esta Directiva vigente desde 1995 se encontraba obsoleta y sobrepasada por la gran evolución tecnológica desde que se creó[72], por lo que la implantación del Nuevo Reglamento Europeo, que más adelante veremos, intenta solventar este "anacronismo".

3.1.2 Nuevo Reglamento General de Protección de Datos (2016/679 de 27 de abril de 2016, RGPD)

Este trabajo no podría haberse realizado en mejor momento, ya que nos encontramos en pleno cambio de legislación europea, una nueva legislación en forma de Reglamento.

Este nuevo Reglamento fue publicado por la Comisión Europea el 25 de enero de 2012 y entró en vigor el 25 de mayo de 2016, pero no ha sido de aplicación hasta el pasado 25 de mayo de 2018 y deroga a la Directiva 95/46. Este período entre la entrada en vigor y su aplicación se ha realizado para permitir que los Estados miembros de la UE, así como sus instituciones y empresas, pudieran ir adaptándose a los cambios que este reglamento introduce.[73] Como bien indica el RGPD en sus considerandos 6 y 7: la gran evolución y revolución tecnológica que se ha realizado en poco tiempo, ha llevado a la necesidad de "*un marco más sólido y coherente para la protección de datos en la Unión Europea"*. El que esta nueva legislación se haya realizado mediante un reglamento, indica que se necesita de una gran uniformidad a la hora de la implantación del derecho a la protección de datos, ya que como reglamento, será directamente aplicable por los Estados miembros y así mejorar el principio de seguridad jurídica. Además, al igual que la anterior

71 C-101/01, 6-11-2003. en los siguientes términos: 1) hacer referencia en una página web a diversas personas e identificarlas, por su nombre o por otros medios, como su número de teléfono, condiciones de trabajo o aficiones, constituye un tratamiento total o parcialmente automatizado de datos personales; 2) un tratamiento de datos consistente en difundirlos por Internet haciéndolos accesibles a un grupo indeterminado de personas ni puede considerarse actividad exclusivamente personal o doméstica ni considerarse exceptuada de la aplicación de la Directiva 95/46 por su art. 3.2. (RALLO, Artemi: *El derecho al olvido en Internet: Google versus España*, cit., pp. 220 a 222)

72 LÓPEZ AQUILAR, Juan Fernando: *Data protection package y parlamento europeo,* en A. RALLO y R. MAHAMUT (dir), cit, p. 49

73 AEPD: http://www.agpd.es/portalwebAGPD/temas/reglamento/index-ides-idphp.php

Directiva, este reglamento es de aplicación exclusivamente para personas físicas y no jurídicas.

Novedades del RGPD:

- Un artículo a tener en cuenta del RGPD es el 3, sobre el ámbito territorial, donde se establece que la normativa se aplicará también a los responsables de tratamiento de datos que, a pesar de no tener un establecimiento en Europa, dirijan sus ofertas de bienes o servicios a ciudadanos de la UE o que controlen su comportamiento.[74] Prácticamente un mes antes de la entrada en vigor del RGPD se publicó una corrección de errores del RGPD[75], donde se indicaba que el RGPD se aplicaba a quien "resida" en la UE, ahora es "que se encuentren".[76]

- Se puede ver en su art. 4 un listado muy actualizado de conceptos que han ido apareciendo con los grandes avances tecnológicos y que eran necesarios delimitar para tener un mejor conocimiento a la hora de la aplicación de la legislación.

- El consentimiento (art. 7) deberá ser demostrado por el responsable del tratamiento de los datos personales, además ahora debe darse mediante un acto claro y explícito (deberá ser expreso), solicitándose con un lenguaje claro y sencillo para su entendimiento fácil. Y se hace una mención expresa al consentimiento otorgado por los menores de 16 años, que solo se considerará lícito si fue autorizado por el titular de la patria potestad o tutela del menor. (art. 8).

- Se ha añadido en el art. 9, donde se indican los datos personales de especial protección, "*el tratamiento de datos genéticos y datos biométricos dirigidos a identificar de manera unívoca a una persona física."* Los datos biométricos consideramos que ha sido interesante que lo tuvieran en cuenta, ya que ha sido un avance tecnológico que está siendo muy utilizado hoy en día.

74 ARENAS, Mónica: *Reforzando el ejercicio del derecho a la protección de datos personales: viejas y nuevas facultades,* en A. RALLO y R. MAHAMUT (dir), cit, p. 321

75 BOE: *http://www.boe.es/buscar/doc.php?id=DOUE-L-2018-80845*

76 En este documento de corrección de errores, en su versión española, se corrigen los considerandos 23, 24, 71 y 80; y los artículos 3.2; 9.1; 37.1.c); 41.3 y 5; 42.7; 43.3 y 6; 57.1.p); 64.1.c), 6, 7 y 8; 65.1.a); 69.2 y 70.1.l), o) y p).

- Los principios que incorpora este Reglamento son el de: licitud, lealtad y transparencia (art. 5), y privacidad desde el diseño y por defecto (art. 25)[77], además del principio de calidad.

- Pretenden dotar al individuo de un poder de control y disposición de sus datos personales.[78] Antes de la implantación del RGPD, los textos internacionales y nacionales únicamente han considerado una modalidad de derecho de cancelación de datos, pero éste no ha satisfecho en la práctica como hubiera sido necesario[79]. Sobre todo mediante un aspecto muy importante que se introduce, el derecho al olvido (art. 17), que exige que ciertas informaciones, pasado un tiempo, sean eliminadas, permitiendo recuperar cualquier dato, y cualquier persona puede ejercer este derecho en el momento que considere oportuno. El derecho al olvido tiene, sin embargo, unas limitaciones y se remite a la legislación aplicable a cada caso.[80] A los derechos ARCO se unen nuevos derechos que son: el derecho de supresión (o derecho al olvido), derecho a la limitación del tratamiento y derecho a la portabilidad de los datos[81]. En la sentencia anteriormente vista de la AEPD vs Google[82], es la primera vez que un tribunal nacional plantea el reconocimiento del derecho al olvido como una cuestión prejudicial al TJUE. Finalmente en la sentencia se concluye que existe un derecho al olvido y que los gestores de los motores de búsqueda son los responsables de borrar la información requerida, incluso cuando la página que la contiene no lo haya hecho; por lo que el afectado podrá dirigirse directamente al gestor del motor de búsqueda para ejercer ese

77 La protección por defecto se refiere a la exigencia de que los parámetros por defecto sean aquellos que proporcionen más protección y menor visibilidad a los datos del individuo, garantizando así que los contenidos no puedan hacerse públicos a priori. La protección desde el diseño es para fomentar el uso de las tecnologías respetuosas con la salvaguarda de la esfera privada, minimizando el almacenamiento de información personal y garantizar que las medidas de protección de datos se incorporan desde la etapa de planificación y desarrollo de cada programa. NOAIN SÁNCHEZ, Amaya: *La protección de la intimidad y vida privada en Internet: la integridad contextual y los flujos de información en las redes sociales (2004-2014)*, cit., p. 118

78 GARRIGA DOMÍNGUEZ, Ana, *Nuevos retos para la protección de datos personales. En la Era del Big Data y de la computación ubicua*, cit. p. 235.

79 RALLO, Artemi: *El derecho al olvido en Internet: Google versus España*, cit., p. 30

80 GARRIGA DOMÍNGUEZ, Ana, *Nuevos retos para la protección de datos personales. En la Era del Big Data y de la computación ubicua*, cit., pp. 215 y 219.

81 Nuevo derecho que se incorpora en su art. 18, que permite obtener una copia de los datos personales y llevarlo a otro responsable de tratamiento de datos. GARRIGA DOMÍNGUEZ, Ana, *Nuevos retos para la protección de datos personales. En la Era del Big Data y de la computación ubicua*, cit. p. 241.

82 Sentencia de 29 de diciembre de 2014 de la AN.

derecho a la retirada de la información.[83] La AEPD considera que el derecho al olvido no está considerado un derecho autónomo de los derechos ARCO, sino la consecuencia de la aplicación del derecho al borrado de los datos personales[84] y que la clave de la verdadera garantía efectiva del derecho al olvido en Internet residía tanto en suprimir información personal en sitios web, como en evitar su indexación en los motores de búsqueda y prohibir su conservación y uso por parte de terceros.[85]

El derecho al olvido en Internet tiene su aspecto más conflictivo en los medios de comunicación, debido a una gran colisión entre el derecho a la protección de datos, el derecho a la libertad de expresión y el derecho a la información.[86] Se debe aplicar el principio de proporcionalidad a cada caso para ver hasta donde llega cada uno de estos derechos. El derecho al olvido se encuentra con un límite, los datos de los personajes públicos, como indicó finalmente el Tribunal Supremo[87] en su sentencia del 4 de abril de 2018[88].

- Se hace una especial mención a la toma de decisiones automatizadas y la creación de perfiles en el art. 22.

- Muy importante es lo que se indica en el art. 31 RGPD, donde se insta a la cooperación de las autoridades de control de los Estados miembros, para que exista una sinergia entre las diferentes autoridades para poder solventar graves riesgos para la protección de datos personales.

- Se impone al responsable la obligación de informar a la Autoridad de Protección de Datos competente sobre las violaciones de seguridad que se pudieran producir en el tratamiento de los datos personales y que se deberá notificar en un plazo no superior a 72 horas (art. 33 RGPD).[89]

---

83 ARENAS, Mónica: *Reforzando el ejercicio del derecho a la protección de datos personales: viejas y nuevas facultades*, en A. RALLO y R. MAHAMUT (dir), cit, pp. 337 a 339

84 Guía del Reglamento de Protección de Datos para responsables de tratamiento que se puede ver en: *http://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/guia_rgpd.pdf#Gu%C3%ADa%20del%20Reglamento%20General%20de%20Protecci%C3%B3n%20de%20Datos%20para%20responsables%20de%20tratamiento*

85 RALLO, Artemi: *El derecho al olvido en Internet: Google versus España*, cit., p. 40

86 RALLO, Artemi: *El derecho al olvido en Internet: Google versus España*, cit., p. 113

87 El economista: *http://www.eleconomista.es/legislacion/noticias/9060579/04/18/El-Supremo-rechaza-conceder-el-derecho-al-olvido-a-personas-publicas.html*

88 Procedimiento 4083/2017.

89 ARENAS, Mónica: *Reforzando el ejercicio del derecho a la protección de datos personales: viejas y nuevas facultades*, en A. RALLO y R. MAHAMUT (dir), cit, p. 354

- Designación de un delegado de protección de datos (DPO) (arts. 37 y ss RGPD) como órgano responsable de velar por la protección de datos personales en una empresa[90]. Lo que cabe reseñar es que este delegado de protección de datos, deberá desempeñar sus funciones manteniendo el secreto de sus funciones; además estará en contacto y en cooperación directa con la autoridad de control, en el caso de España, la AEPD. Y encontraremos en este art. 37.1 las organizaciones que estarán obligadas a contratar un DPO para supervisar el tratamiento de los datos que se realicen[91].

- En el considerando 84 y en el art. 35 RGPD se establece que se lleve a cabo una evaluación de impacto de la protección de datos evaluando el riesgo para los derechos y libertades de la persona afectada, esta evaluación la debe realizar el responsable del tratamiento de los datos.

- Art. 40 promueve la elaboración de códigos de conducta para contribuir a la correcta aplicación del Reglamento[92], promoviendo la autorregulación.

- El régimen de transferencia de datos a terceros países que estaba establecido con la Directiva 95/46 era muy débil, sin embargo con el nuevo RGPD, todas las transferencias deberán limitarse a las indicadas en dicho Reglamento y siempre que el encargado del tratamiento asegure las garantías adecuadas para la protección de datos personales (arts. 44 y ss RGPD).[93]

- El RGPD contiene un nuevo régimen sancionador muy elevado, que contempla unas infracciones y sanciones administrativas de cuantía muy elevada para los responsables de datos.

---

90 AGUSTINA, José y BLUMENBERGU, Axel-Dirk: *El Data Protection Officer en el marco de la responsabilidad penal de las personas jurídicas. Consideraciones a la luz del nuevo Reglamento Europeo en materia de protección de datos,* en A. RALLO y R. MAHAMUT (dir), cit., p.247

91 Será obligatorio la figura del DPO en las autoridades y organismo públicos, en los responsables o encargado que tengan entre sus actividades principales las operaciones de tratamiento que requieran una observación habitual y sistemática de interesados a gran escala; y en los responsables o encargados que tengan entre sus actividades principales el tratamiento a gran escala de datos sensibles. Encontrado en AEPD: *Guía del Reglamento General de Protección de Datos para Responsables de Tratamiento: https://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/guia_rgpd.pdf*

92 Los códigos de conducta son documentos que una organización expone dando a conocer a terceros prácticas, principios o derechos que se comprometen a respetar unilateralmente. Es necesaria la previa autorización por la correspondiente agencia de protección de datos. VIGURI, Jorge: *Los mecanismos de certificación (códigos de conducta, sellos y marcas)*, en A. RALLO y R. MAHAMUT (dir), cit., pp. 912 y 913

93 LÓPEZ AGUILAR, Juan Fernando: *Data protection package y parlamento europeo,*en A. RALLO y R. MAHAMUT (dir), cit., p.47

- Inclusión del ámbito laboral en el art. 88 RGPD, que no había sucedido hasta este momento y que requerirá de un gran desarrollo en la ley nacional o en convenios colectivos.

3.2. Normativa nacional

3.2.1. Constitución Española de 1978

Nuestra Constitución es una de las primeras en introducir la protección de los datos frente al uso de Internet.[94] Además, encontramos que la dignidad de la persona se muestra como el contenido esencial de nuestra Constitución.[95]

La CE de 1978 hace referencia en su sección 1ª: *"De los derechos fundamentales y de las libertades públicas",* a los diferentes conceptos que nos encontramos en este trabajo, clasificándolos como derechos fundamentales. Principalmente, su art. 18.1 donde se hace referencia al "*derecho al honor, a la intimidad personal y familiar y a la propia imagen"*, consagrando así el derecho a la intimidad como derecho fundamental. En el art. 18.4 vemos como se establece que *"la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos"*. En este último artículo vemos que la CE intenta establecer o que deriva de una manera muy difusa un derecho a la protección de datos personales, libertad o autodeterminación informativa, libertad informática o *habeas data*[96].[97] Además de estos derechos fundamentales, que son en los que se centra este trabajo, nos encontramos con los derechos fundamentales de los arts. 14 a 29 CE. Todos los derechos fundamentales que contiene nuestra Constitución atienden a la necesidad de crear y mantener las condiciones mínimas para que el desarrollo de la libertad y la dignidad de la persona sean efectivas.[98]

---

94 Sipnosis artículo 18 de la Constitución Española: *http://www.congreso.es/consti/constitucion/indice/sinopsis/sinopsis.jsp?art=18&tipo=2*, 2011

95 REBOLLO DELGADO, Lucrecio: *El derecho fundamental a la intimidad*, 2ª ed, Dykinson, Madrid, 2005, p. 110

96 El habeas data es el derecho que tiene toda persona para conocer, actualizar y rectificar toda aquella información que se relacione con ella y que se recopile o almacene en centrales de información. Extraído de SERFINASA: http://www.serfinansa.com.co/servicioclientе/leyhabeasdata

97 HERNÁNDEZ LÓPEZ, José Miguel: *El Derecho a la Protección de Datos Personales en la Doctrinal del Tribunal Constitucional*, cit., p. 29.

98 REBOLLO DELGADO, Lucrecio: *El derecho fundamental a la intimidad*, cit, p. 114

De los arts. 10 y 18.4 CE deriva el derecho fundamental a la protección de datos de carácter personal, que ha sido definido como autónomo e independiente por las SSTC 292/2000, de 30 de noviembre[99] y 254/1993, de 20 de julio. La CE también hace referencia a la especial protección para los datos denominados sensibles, como son los que afectan a la ideología, religión o creencias, referidos en el art. 16.2 CE. A todo esto, hay que añadir que los derechos que se encuentran en el art. 18 CE están sometidos a reserva de ley orgánica (art. 81 CE).[100]

Estos derechos fundamentales gozan de diferentes medidas de protección que se recogen en la misma CE: 1. cualquier ciudadano puede solicitar la tutela de estos derechos fundamentales ante los Tribunales ordinarios, por un procedimiento basado en los principios de preferencia y sumariedad (art. 53.2 CE). 2. Acudir al recurso de amparo ante el TC (arts. 53.2 y 161.1.b) CE). 3. Cabe recurso de inconstitucionalidad contra las Leyes y disposiciones normativas con fuerza de ley que vulneren estos derechos fundamentales (arts. 53.1 y art. 161.1.ª) CE). 4. Acudir al defensor del Pueblo, art. 54 CE.[101]

Podemos ver también que la Constitución Europea ha mencionado expresamente el derecho fundamental a la protección de datos en dos ocasiones, en la Parte I, TítuloVI, el artículo I-51[102] y en la Parte II, Título II, art. II-68.[103]

---

99 AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD): *Guía del Derecho Fundamental a la Protección de Datos de Carácter Personal*, 2004. https://www.agpd.es/portalwebAGPD/common/FOLLETO.pdf, p. 7

100 Sinopsis artículo 18 de la Constitución Española: *http://www.congreso.es/consti/constitucion/indice/sinopsis/sinopsis.jsp?art=18&tipo=2*, cit.

101 FUNDACIÓN HUMANA PRO DERECHOS HUMANOS: *http://www.derechoshumanos.net/constitucion/articulo18CE.htm*

102 Establece en el epígrafe primero que "*toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan"*

103 Señala que *"toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan"* y que *"estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo por la ley"*, además de que *"toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a obtener su rectificación"*. AEPD: *Guía del Derecho Fundamental a la Protección de Datos de Carácter Personal*, cit. p. 8

3.2.2 Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (LOPD) y su Reglamento de desarrollo RD 1720/2007, de 21 de diciembre (RLOPD)

En España, la Ley Orgánica 5/1992 (LOTARD) fue sustituida en muy poco tiempo por la LO 15/1999. La Directiva 95/46 fue transpuesta a través de esta LOPD, con la que guarda muchas similitudes. Debido a la velocidad de los avances tecnológicos, se sintió la necesidad de modificar esta Ley, por lo que se probó en 2007 el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de Desarrollo de esta Ley Orgánica (RLOPD). Tras la aplicación del nuevo RGPD, la LOPD seguirá siendo de aplicación en lo que no se oponga al RGPD hasta que se instaure la nueva LOPD de la que hablaremos más adelante.

Como hemos indicado, la Ley española ha sido muy conforme a la Directiva 95/46, haciendo una aplicación de la Directiva bastante directa, como por ejemplo, la LOPD, al igual que la Directiva 95/46, limita la protección de los datos personales a las personas físicas. Lo que entendemos razonable, debido que los derechos que se protegen son solo exigibles por personas físicas y no personas jurídicas.

La LOPD, antes de la instauración del nuevo RGPD, constituía la ley general en materia de protección de datos, aunque existe una gran cantidad de normativa sectorial que regula el tratamiento de los datos de carácter personal en ámbitos más específicos[104], como la Ley 9/2014 General de Telecomunicaciones, o la Ley 34/2002 de servicios de la sociedad de la información y de comercio electrónico.

La LOPD fue aprobada por las Cortes Generales para garantizar y proteger el derecho a la protección de los datos personales. Es de aplicación a los datos de carácter personal que se registren susceptibles de posterior tratamiento. Mencionaremos los aspectos más importantes que esta LOPD integra en la legislación nacional, como los derechos que recoge para los afectados por las intromisiones a los datos personales. Entre estos derechos nuevos nos encontramos con la incorporación de los derechos ARCO,

104 HERNÁNDEZ LOPEZ, José Miguel: *El Derecho a la Protección de Datos Personales en la Doctrina del Tribunal Constitucional*, cit, p. 56

derechos de acceso (art. 15 LOPD), rectificación (art. 16 LOPD), cancelación (art. 16 LOPD) y oposición (art. 6.4 LOPD). Otros derechos que vemos recogidos son los derechos a la impugnación (art. 13 LOPD), indemnización (art. 19 LOPD) y de consulta al Registro General de Protección de Datos[105] (art. 14 LOPD).[106]

Un aspecto muy importante tratado en esta LOPD es el de toma decisiones automatizadas de su art. 13.1 (y art. 15.1 de la Directiva 95/46), donde podemos ver que este aspecto es reprochable, sobre todo, cuando tenga efectos jurídicos. Se aprecia en esta norma que el tratamiento de datos personales ha de realizarse de acuerdo con los principios de:[107]

- Calidad (art. 4 LOPD), los datos de carácter personal recogidos 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"*. Todo esto aplicando el principio de proporcionalidad.

- Información (art. 5 LOPD), se debe informar previamente *"de modo expreso, preciso e inequívoco"* a la recogida de datos para que el propietario de éstos pueda tener conocimiento en todo momento de su situación.

- Consentimiento (art. 6 LOPD), nos encontramos con un concepto muy determinante e importante en este trabajo. El consentimiento es la base de toda recogida de datos y existe un gran debate de cómo debe ser éste y cómo se debe solicitar. Un aspecto muy importante a tener en cuenta sobre el consentimiento es el que recoge el art. 13 RLOPD, donde se indica el caso especial del consentimiento para el tratamiento de datos de menores de edad.

- Seguridad (art. 9 LOPD): se obliga al responsable del fichero, o encargado de su tratamiento, a adoptar toda clase de medidas de seguridad para adoptar el correcto tratamiento de estos datos, tanto en la recogida, como

105 HERNÁNDEZ LOPEZ, José Miguel: *El Derecho a la Protección de Datos Personales en la Doctrina del Tribunal Constitucional*, cit, p. 56

106 Este Registro es el órgano creado por la AEPD, como figura en su página web, al que corresponde velar por la publicidad de la existencia de los ficheros y tratamientos de carácter personal. AEPD: *https://www.agpd.es/portalwebAGPD/canalresponsable/inscripcion_ficheros/index-ides-idphp.php*

107 HERNÁNDEZ LOPEZ, José Miguel: *El Derecho a la Protección de Datos Personales en la Doctrina del Tribunal Constitucional*, cit, p.69

en el almacenamiento, en su tratamiento y finalmente en su borrado tras no necesitarlos más.

- Secreto (art. 10 LOPD): se exige al responsable del fichero el secreto profesional respecto de los datos personales que tenga en su poder, incluso después de que este responsable ya no disponga de los datos.

En el art. 7 LOPD nos encontramos con la introducción de los datos de especial protección, que son los datos sobre ideología, religión, afiliación sindical, creencias, salud y vida sexual. De estos datos se requiere un consentimiento expreso y por escrito, además que el individuo no tiene por qué prestar esta información. Este aspecto es muy importante, ya que ha sido un aspecto que se le ha recriminado en numerosas ocasiones a la red social Facebook.

La LOPD fue sometida a un recurso de inconstitucionalidad de alguno de sus artículos. El 14 de marzo de 2000[108], el Defensor del Pueblo interpuso recurso de inconstitucionalidad contra los arts. 21.1. y 24.1 y 2 de la LOPD, ya que alegaba que vulneraban los derechos fundamentales del art. 18.1, en relación con su apartado 4 CE, y la reserva de ley del art. 53.1 CE, es decir, los derechos fundamentales al honor, a la intimidad personal y familiar y a la propia imagen. Finalmente se declaró nulo e inconstitucional el apartado 1 del art. 21 de la LOPD[109] y el apartado 1 del art. 24[110] y todo su apartado 2. Esta sentencia es también muy importante en cuanto a la determinación del derecho a la protección de datos como derecho autónomo, que veremos con más detenimiento en el epígrafe 4.4.

En cuanto al RLOPD, nos encontramos con que su art. 10 fue sometido a un recurso ante el Tribunal Supremo[111], ya que FECEMD (Federación Española de la Economía Digital, ahora adigital) consideró que el art. 10.2 a), supuesto primero, y 2.b), párrafo primero; eran contrarios al art. 7.f) de la

108 Sentencia 292/2000 del Tribunal Constitucional.

109 El inciso que indica: "c*uando la comunicación hubiere sido prevista por las disposiciones de creación del fichero o por disposición de superior rango que regule su uso"*

110 Los incisos donde se indica: "*impida o dificulte gravemente el cumplimiento de las funciones de control y verificación de las Administraciones públicas*" y "*o administrativas*".

111 Sentencia de 8 de febrero de 2012 del tribunal Supremo (RJ 2012/291)

Directiva 95/46.[112] El TS planteó 2 cuestiones prejudiciales al TJUE[113], estableciendo finalmente que la Directiva 95/46 realiza un listado cerrado y que los Estados miembros no pueden ampliar este listado. Finalmente el TS, tras la consulta al TJUE, declaró nulo el art. 10.2.b) por ser contrario al artículo citado de la Directiva 95/46. Y, aunque el art. 6.2 LOPD también resultaría contrario a la Directiva 95/46, el Tribunal Supremo carece de competencia para anular disposiciones que tengan rango de ley, por lo que este precepto de la LOPD sigue vigente.[114]

3.2.3. Proyecto de la nueva Ley Orgánica de Protección de Datos española

Actualmente hay un proyecto de una nueva LOPD para completar el RGPD en los aspectos que este no contemple, a pesar de no necesitar transposición, y que derogaría la actual LOPD. Todavía se desconoce cuándo entrará en vigor y cuál será su contenido completo, ya que está sometida a una gran cantidad de enmiendas.

El 10 de noviembre de 2017 el Consejo de Ministros aprobó el anteproyecto de Ley Orgánica de Protección de datos para adaptar el RGPD a nuestra legislación, después de obtenerse los informes de impacto y el Dictamen del Consejo de Estado, se convirtió en el actual Proyecto de Ley. Posteriormente se presentó ante el Congreso de los Diputados empezando su tramitación parlamentaria, en la votación plenaria de la enmienda total de la ley (16 si, 318 no y 7 abstenciones)[115] y se abrió paso a las enmiendas. Finalmente el 18 de abril se publicaron en el BOE las enmiendas a este Proyecto de Ley.[116]

---

112 En estos arts. Del RLOPD se establecen una serie de supuestos en los que es posible el tratamiento o cesión de datos personales sin el consentimiento del interesado. En el art. 7.f) de la Directiva 95/46 se establece que el tratamiento de datos personales solo puede efectuarse si *"es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección con arreglo al apartado 1 del artículo 1 de la presente Directiva."*

113 Sentencia de 24 de noviembre de 2011 del Tribunal de Justicia de la Unión Europea sobre cuestiones prejudiciales planteadas.

114 FERNÁNDEZ-SAMANIEGO, Javier y FERNÁNDEZ-LONGORIA, Paula: *El interés legítimo como principio para legitimar al tratamiento de datos*, en A. RALLO y R. MAHAMUT (dir), cit, pp. 416 y ss.

115 Elderecho.com: *http://tecnologia.elderecho.com/tecnologia/privacidad/tramitacion-LOPD-Congreso-proteccion-datos_11_1197055003.html*

La creación de esta Ley nacional es importante debido a que el RGPD exige en ciertos aspectos un desarrollo por parte de la legislación nacional, como es el caso de determinar la edad para considerar a menores en el tratamiento de sus datos personales, así como el tratamiento de los datos personales de los trabajadores en el RGPD que se ha introducido como novedad (a lo que no hace referencia el actual Proyecto de LOPD).

Este Proyecto de LOPD contiene 78 artículos que realiza bastantes remisiones al RGPD ya que nos encontramos ante una norma de desarrollo o un complemento al RGPD que lo. La incertidumbre de cuándo entrará en vigor estando ya en vigor el RGPD, provoca una sensación de inseguridad jurídica, sobre todo en el aspecto de que no hay un claro procedimiento a seguir para resolver los expedientes y sanciones administrativas de las violaciones de protección de datos.

En este Proyecto de LOPD se determina la edad de 13 años para limitar la licitud de su consentimiento. Además se hace mención al sistema de videovigilancia ampliamente (art. 22), tanto en el ámbito de la vía pública, siempre que sea necesario y con su eliminación en el plazo máximo de un mes; como en el ámbito laboral e informando acerca de esta medida de seguridad, pero indica que si se hubieran captado actos delictivos, la no información, no invalidará la prueba de esta grabación. Este aspecto es muy importante, ya que se a lo largo de los años se han producido muchas dudas sobre si la no información podría producir la invalidez de esta prueba. Aunque finalmente veremos cómo acaba este proceso a una nueva LOPD y el contenido exacto de ésta.

3.2.4. Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones y su Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006 de Retención de Datos

Aunque la Directiva 2006/24/CE fue anulada por el TJUE el 8 de abril de 2014[117] por resultar contraria a la Carta de Derechos Fundamentales de la UE,

116 BOE 18 abril 2017: *http://www.congreso.es/public_oficiales/L12/CONG/BOCG/A/BOCG-12-A-13-2.PDF*

117 Sentencia C-293/12

la Ley 25/2007 que la transpuso sigue vigente y haremos una revisión de lo que suponía la Directiva y lo que mantiene la ley actual española de Conservación de Datos relativos a las comunicaciones electrónicas y las redes públicas de comunicaciones.

En cuanto a la información que se almacena por las empresas o entidades, nos encontramos con que tienen una "aliada". La Directiva de 2006 de la UE de Retención de Datos. En esta ley, como indica en su artículo 5, "permite" a los operadores que presten servicios[118] de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones, conservar los datos de esas comunicaciones durante un período mínimo de 6 meses y de un máximo de 2 años, que podrán ser entregadas "*a los agentes facultados*" y "*previa autorización judicial"*, según se indica en su artículo 6.

El TJUE en la sentencia donde se invalidó esta Directiva, afirmó que la privacidad y la confidencialidad de las comunicaciones deben prevalecer sobre cualquier práctica de retención masiva y desproporcionada de datos personales, incluso cuando el argumento sea mejorar la seguridad de los ciudadanos. Afirma también que el derecho a retener los datos debe hacerse de forma proporcional, limitada y con un fin concreto[119]. Lo que ha llevado a este comportamiento legislativo son los terribles atentados producidos, modificando los estándares de seguridad y las exigencias que se derivan, poniendo en riesgo el ejercicio de otros derechos, como el de protección de datos personales, y prueba de esta tensión entre seguridad y protección de datos es esta Directiva 2006/24/CE.[120]

---

118 Se consideran prestadores de servicios de la sociedad de la Información, conforme a la Exposición de Motivos de la Ley 34/2002, de servicios de la sociedad de la información y de comercio electrónico: a los operadores de telecomunicaciones, los proveedores de acceso a Internet, los portales, los motores de búsqueda y cualquier sujeto que disponga de un sitio en Internet.

119 LÓPEZ AGUILAR, Juan Fernando: *Data protection package y parlamento europeo,* en A. RALLO y R. MAHAMUT (dir), cit., pp. 79 y 80

120 MURILLO DE LA CUEVA, Pablo Lucas y PIÑAR MAÑAS, José Luis: *El derecho a la autodeterminación informativa*, cit., pp. 148 y 149

4. APLICACIÓN DE LA LEGISLACIÓN A LOS CONCEPTOS DEL *BIG DATA*

4.1. Figuras en materia de protección de datos y sus derechos y deberes en la relación con el *big data*

Cuando hablamos de la protección de los datos personales y su tratamiento nos encontramos diferentes partes que intervienen en este proceso: el interesado, el responsable del tratamiento, el encargado del tratamiento y el destinatario de estos datos personales. Todos estas partes tienen una serie de deberes y derechos que pueden exigir cuando consideren necesario.

En el RGPD encontramos una clara definición de todos ellos en su art. 4. El responsable del tratamiento es la persona física o jurídica que determina los fines y los medios de recogida de los datos personales; y el encargado del tratamiento es la persona (física o jurídica) encargada de llevar a cabo el tratamiento de los datos personales recogidos. El interesado es el titular de esos datos personales. Y finalmente el destinatario es la persona física o jurídica receptora de esos datos personales, pudiendo ser un tercero.

Cuando hablamos de los derechos y deberes de los interesados nos encontramos con que la LOPD les reconoce el derecho a la información en la recogida de datos, derecho de consulta al registro general de protección de datos[121]; y los conocidos derechos ARCO, junto con los nuevos derechos recogidos en el RGPD del derecho al olvido, la limitación del tratamiento y derecho a la portabilidad de los datos. El interesado puede ejercer estos derechos ante el responsable de un fichero o del tratamiento con el fin de conocer sus datos personales para solicitar que sean modificados o cancelados, o bien para oponerse a su tratamiento.[122] Gracias a estos nuevos derechos, cuando se solicitan los datos a un interesado, el responsable debe informar de qué datos se recogen, para qué se van a utilizar y cuál va a ser su

121 Se permite a los interesados conocer de la existencia de un fichero o tratamiento de datos dirigiéndose a la AEPD.

122AEPD: *Guía del Derecho Fundamental a la Protección de Datos de Carácter Personal*, cit. pp. 15 y 16.

destinatario, obteniendo todo esto mediante un consentimiento libre, expreso y específico para cada aspecto de su tratamiento posterior.

Cuando se ejerce el derecho al olvido hay que tener en cuenta que, por la características que tiene el mundo tecnológico, aun cuando un prestador de servicios de la Sociedad de la Información retira contenido, éstos pueden seguir en Internet durante un tiempo indeterminado, ya que esta información se puede guardar en los buscadores y en la memoria denominada caché, que permite que los contenidos puedan permanecer en la web sin control alguno[123], por lo que si no tenemos claro la cantidad de información que hay en la Web sobre nosotros, podremos solicitar ayuda a la AEPD.

Con la implantación del nuevo RGPD, los interesados pueden exigir directamente ante los tribunales su cumplimiento, procedimiento de reclamación que quedará más aclarado con la entrada en vigor de la nueva LOPD.

Todos estos derechos de los interesados se encuentran con la limitación de respetar el resto de derechos como el de información o la libertad de expresión.

En el ámbito de los responsables, encargados del tratamiento y destinatarios nos encontramos con que éstos suelen tener más obligaciones que derechos. Todo responsable de un fichero o tratamiento de datos personales está obligado a cumplir con los principios de información, calidad, finalidad, consentimiento, seguridad, licitud, lealtad y transparencia que recogen la LOPD y el RGPD. Además, todo responsable o encargado de un tratamiento tiene que adoptar las medidas necesarias para garantizar la seguridad de los datos personales e impedir cualquier alteración, pérdida, tratamiento o acceso no autorizado, igual que notificar al Registro General de Protección de Datos la creación, modificación o supresión de cualquier fichero o tratamiento de datos personales.[124] Del mismo modo, las organizaciones deberán añadir la figura del DPO para la supervisión del tratamiento que hagan de los datos que se regula en el RGPD; debiendo, además, adoptar los, ya

123 GARRIGA DOMÍNGUEZ, Ana, *Nuevos retos para la protección de datos personales. En la Era del Big Data y de la computación ubicua*, cit. p. 120.

124 AEPD: *Guía del Derecho Fundamental a la Protección de Datos de Carácter Personal*, cit. pp. 12 y 13

mencionados, mecanismos de protección de los datos por defecto y desde el diseño.

En el caso de que, a pesar de llevar a cabo las medidas necesarias para la protección de los datos personales, se produzca una violación o brecha de seguridad, el responsable del tratamiento debe notificar a la autoridad de control competente en un plazo máximo de 72 horas, así como al encargado del tratamiento y al interesado.

Según la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información (LSSI), en su art. 13.1 se establece que *"los prestadores de servicios de la Sociedad de la Información están sujetos a la responsabilidad civil, penal y administrativa establecida con carácter general en el ordenamiento jurídico"*. En esta ley se indica que la responsabilidad de los prestadores de servicios de la sociedad de la información se centra en aquellos contenidos que ellos mismos elaboren o que se hayan elaborado por cuenta suya, mientras que no serán responsables por las actividades de intermediación, y en los términos de los arts. 13 a 17, la transmisión, copia, almacenamiento o localización de contenidos ajenos.[125]

Es importante que las organizaciones y empresas encargadas de tratamiento de datos tengan una estructura precisa para poder evaluar los riesgos que supone la exposición de los datos al dominio público.[126] El código de buenas prácticas sobre la anonimización es un ejemplo de como Reino Unido ha creado una guía de ayuda para las empresas en el trato de información o datos personales obtenidos en su actividad empresarial, sin embargo este código de buenas prácticas no es de cumplimiento obligatorio y se debe suplir con el *Data Protection Act* (DPA) de 1998, que es quien impone obligaciones legalmente exigibles a las organizaciones[127].

A pesar de todos los esfuerzos que las diferentes leyes e instituciones hacen día a día para la protección de los datos personales, los datos no tienen

125 DRUMMOND, Víctor y traducción de ESPÍN ALBA, Isabel: *Derecho de las nuevas tecnologías*, cit., p.93.

126 INFORMATION COMMISSIONER'S OFFICE (ICO): <<*Anonymisation: managing data protection risk code of practice*>>, 2012: https://ico.org.uk/media/1061/anonymisation-code.pdf. ICO es el organismo independiente del Reino Unido creado para defender los derechos de información.

127 ICO: «Anonymisation: managing data protection risk code of practice*», cit*.

país y en la era tecnológica no hay fronteras geográficas, por lo que los datos fluyen libremente[128] y es complicado aplicar la legislación en muchos casos. Finalmente, podemos encontrar un mayor desarrollo de cómo los Responsables de tratamiento de datos personales deben incorporar el RGPD en su política en la Guía del RGPD para Responsables de Tratamiento para un correcto desarrollo de su actividad y no incurrir en el cuantioso régimen sancionador del RGPD.[129]

4.2. La importancia del consentimiento en el *big data*

La definición de consentimiento del interesado la encontramos en el art. 4 del RGPD, donde se indica que es "*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".* Como vemos también en el art. 7 de este mismo Reglamento, se indica que el consentimiento debe ser expreso. La inclusión de unos datos personales en un fichero, requerirá el consentimiento del afectado.[130] El consentimiento sale reforzado con el RGPD.

Corresponderá al titular de los datos determinar cuáles de sus datos pueden ser registrados y tratados, y el uso que se va a dar de ellos, para ello, resulta imprescindible que previamente se haya cumplido la exigencia de información de "*modo expreso, preciso e inequívoco"*, como indica el art. 5.1 LOPD. Ya que, además, para autorizar el tratamiento de sus datos, ha de conocer las consecuencias y finalidades que se derivan del mismo y que debe

128 Un ejemplo de esto es la admisión de Microsoft de que los datos almacenados en sus servidores europeos pueden ser entregados a los investigadores estadounidenses sin informar al individuo. Esto es una violación de la Directiva de Protección de Datos de la UE y del acuerdo de Puerto seguro con los EEUU. La Ley Patriota prevalece sobre cualquier otra legislación de privacidad, independientemente de dónde se originaron o dónde residen los datos. (CRAIG, Terence y LUDLOFF, Mary E.: *Privacy and Big Data,* cit. Chapter 2). Sin embargo, Microsoft sigue luchando contra esta situación y quiere impedir que las autoridades de los EEUU accedan a los datos que esta empresa almacene en otros países y todo empezó cuando Microsoft se negó a entregar los datos de una cuenta de correo electrónico cuyos datos se encontraban almacenados en un servidor en Dublín, Irlanda, cuyo caso está a la espera de la resolución de una apelación por parte de la administración de Donald Trump. (GENBETA: https://www.genbeta.com/actualidad/microsoft-quiere-impedir-que-las-autoridades-de-estados-unidos-accedan-a-datos-que-almacenan-en-otros-paises).

129 AEPD: *https://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/guia_rgpd.pdf*

130 HERNÁNDEZ LÓPEZ, José Miguel: *El Derecho a la Protección de Datos Personales en la Doctrinal del Tribunal Constitucional*, cit., pp. 70 y 71

saber con anterioridad a la prestación del consentimiento.[131] Sin embargo, en el art. 7.3 RGPD se indica que el consentimiento se puede retirar en cualquier momento. Existen varios tipo de sistemas para recopilar el consentimiento: el opt-in y el opt-out.[132]

Hoy en día el mayor valor de los macrodatos son sus usos secundarios que son posibles con la obtención de la información de los usuarios. Una vez se tiene la información recopilada es cuando se puede ver el potencial que tiene ésta, por lo que el consentimiento que se otorgue a priori, no tiene el alcance necesario. Por esto, la empresa que haya obtenido esos datos, debería volver a solicitar el consentimiento del individuo en función de las finalidades a que se va a destinar esa información de nuevo, pero este sistema supone un mayor coste para las empresas.[133]

A pesar de todo lo dicho, el gran problema que existe actualmente, es que la mayoría de personas no prestan atención a la hora de prestar su consentimiento y leer las políticas de privacidad, debido a la gran complejidad, por lo que se podría considerar que las relaciones, en estos casos, son desequilibradas.[134]

4.3. La vulneración de la intimidad y la privacidad en el uso del *big data*

Cuando nos relacionamos con las tecnologías de los macrodatos es inevitable que nuestra privacidad e intimidad se vean mermadas debido a que las tecnologías del *big data* se introducen en nuestra vida para saber todo de nosotros y después utilizarlo. No existe un concepto claro del derecho a la intimidad en nuestro Derecho positivo, la CE en su art. 18.1 se limita a consagrarlo como derecho fundamental y como tal, le otorga su protección.[135]

131 GARRIGA DOMÍNGUEZ, Ana, *Nuevos retos para la protección de datos personales. En la Era del Big Data y de la computación ubicua*, cit. pp. 185 y ss.

132 El sistema opt-in se basa en que el usuario debe manifestar un consentimiento expreso y positivo rellenando la casilla creada al efecto. Y en el sistema opt-out, el individuo debe manifestar su oposición, bien rellenando la casilla correspondiente o manifestándolo de otro modo. GIL, Elena, *Big data, privacidad y protección de datos,* cit. p. 79

133 GIL, Elena, *Big data, privacidad y protección de datos,* cit. p.67

134 ÁLVAREZ, Cecilia: *El poder del usuario digital*, en A. RALLO y R. MAHAMUT (dir), cit, p.296 y 301

135 GARRIGA DOMÍNGUEZ, Ana, *Nuevos retos para la protección de datos personales. En la Era del Big Data y de la computación ubicua*, cit. p. 80

Sin embrago, podemos indicar que el derecho a la intimidad es un derecho de la personalidad que tiene por objetivo garantizar al individuo un ámbito reservado de su vida vinculado con el respeto de su dignidad como persona. Su bien jurídico es el respeto a la existencia de un ámbito propio y reservado de la vida frente a la acción y conocimiento de los demás.[136] Si tenemos en cuenta la definición de intimidad de la RAE, la intimidad es la zona espiritual íntima y reservada de un persona o de un grupo, especialmente de una familia.

Cuando hablamos del derecho a la intimidad, es inevitable mencionar el art. 8 del Convenio de Roma de 4 de noviembre de 1950, para la Protección de los Derechos Humanos y de las Libertades Fundamentales que consagra el derecho al respeto a la vida privada y familiar.[137] Pero esto se completa con la regulación del Convenio 108 del Consejo de Europa, de 28 de enero de 1981, para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal, y en su art. 9.2 se dice que la intromisión o excepción de los arts. 5, 6 y 8, solo se podrá realizar cuando "*constituya una medida necesaria en una sociedad democrática"*, ponderando siempre los intereses en conflicto.

Para resolver un posible conflicto entre la libertad de expresión e información con los derechos fundamentales del honor, la intimidad personal y familiar y a la propia imagen del art. 18 CE, se habrá de tener en cuenta la especial posición de las libertades de expresión e información, el requisito de veracidad de la información expuesta, el requisito de interés general o relevancia pública de la información, y la adecuación de las expresiones y términos empleados.[138]

El TC no tiene un concepto claro de derecho a la intimidad, llegando a veces a confundir conceptos con el derecho al honor, a la intimidad y a la propia imagen que se recogen en el art. 18.1 CE.[139] El concepto de vida privada

136 HERNÁNDEZ LÓPEZ, José Miguel: *El Derecho a la Protección de Datos Personales en la Doctrinal del Tribunal Constitucional*, cit., p. 32.

137 GARRIGA DOMÍNGUEZ, Ana, *Nuevos retos para la protección de datos personales. En la Era del Big Data y de la computación ubicua*, cit. p. 78

138 GARRIGA DOMÍNGUEZ, Ana, *Nuevos retos para la protección de datos personales. En la Era del Big Data y de la computación ubicua*, cit. pp. 129 y ss.

139 Sentencia del Tribunal Constitucional STC 121/2002, de 20 de mayo, fundamento jurídico primero. GARRIGA DOMÍNGUEZ, Ana, *Nuevos retos para la protección de datos personales. En la Era del Big Data y de la computación ubicua*, cit. p. 83

es muy amplio y engloba todo aquello que no es, o que no queremos que sea de general conocimiento. Dentro de ésta, existe un núcleo que más protegemos, y esto último es lo que se consideraría intimidad.[140]

No se puede hablar de privacidad sin considerar el contexto en el que nos encontremos, ya que lo que puede ser importante para una persona, puede no serlo para otra. Incluso la cultura desempeña un papel imprescindible en la percepción que se tiene de la privacidad.[141] Mientras los datos personales estén almacenados en el ordenador sin ser utilizados, el sitio web no está violando la privacidad del usuario.[142]

La violación de la privacidad en Internet tiene lugar: 1º) cuando hay un desplazamiento de datos o informaciones de un ambiente de comunicación privada a un ambiente de comunicación pública; o 2º) cuando hay un desplazamiento de datos o informaciones de un ambiente de comunicación privada para un ambiente de comunicación privada del cual el titular de los datos o informaciones no forme parte. Y la autorización del titular para efectuar el desplazamiento, hará que no se produzca una violación.[143]

4.4. Datos personales y anonimización en el contexto del *big data*

Encontramos una definición clara y completa de lo que se consideran los datos personales en el art. 4 del RGPD donde se indica que son datos personales "*toda información sobre una persona física identificada o identificable (el interesado); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica,*

140 REBOLLO DELGADO, Lucrecio: *El derecho fundamental a la intimidad*, cit, p.73
141 CRAIG, Terence y LUDLOFF, Mary E.: *Privacy and Big Data,* cit. chapter 2
142 DRUMMOND, Víctor y traducción de ESPÍN ALBA, Isabel: *Derecho de las nuevas tecnologías*, cit., p. 114
143 DRUMMOND, Víctor y traducción de ESPÍN ALBA, Isabel: *Derecho de las nuevas tecnologías*, cit., p. 45

económica, cultural o social de dicha persona". Se ha considerado que las direcciones IP[144] son datos personales, incluso si son dinámicas.[145]

En el camino a la consagración como derecho fundamental autónomo de protección de los datos personales ocupa un lugar principal la sentencia de 15 de diciembre de 1983, del Tribunal Constitucional Federal alemán, ya que en ella se reconoce por primera vez el derecho a la autodeterminación informativa hasta ese momento invocado por la doctrina.[146] Pero, como todo derecho fundamental, el derecho a la protección de datos personales, no es un derecho absoluto, sino que en ocasiones debe ceder ante otros derechos o bienes constitucionales[147], como puede darse en el caso de la libertad de expresión e información o el principio de publicidad de las resoluciones judiciales, por lo que habrá que estar a las circunstancias concretas de cada caso.[148] Un ejemplo de esto podemos verlo en la STC 17/2013, de 31 de enero.

Como derecho de protección de datos, no existe unanimidad en su fundamento, ya que se debate si deriva del art. 18.4 CE, como se indica en las SSTC 290/2000 y 292/2000, o, por el contrario, tiene su fundamento en el art. 10.1 CE[149]. Estas sentencias son conocidas por ser las primeras en las que se reconoce el derecho a la protección de datos personales como un nuevo derecho fundamental de tercera generación. El bien jurídico de este derecho es el de asegurar a las personas el control de la información que le es propia para protegerles del uso que terceros puedan hacer de esta información.[150]

En el considerando 4 del RGPD vemos como se refuerza el que el derecho a la protección de datos no es un derecho absoluto, sino que debe tener un equilibrio y proporcionalidad con el resto de derechos y aspectos de la

144 Es un número único e irrepetible con el cual se identifica un ordenador conectado a una red que utilice el protocolo IP. En Uservers: *http://web.uservers.net/ayuda/soluciones/dominios/que-es-una-direccion-ip_NTk.html*

145 ÁLVAREZ, Cecilia: *El poder del usuario digital*, en A. RALLO y R. MAHAMUT (dir), cit, p. 288

146 GARRIGA DOMÍNGUEZ, Ana, *Nuevos retos para la protección de datos personales. En la Era del Big Data y de la computación ubicua*, cit. p.92 y 93

147 GARRIGA DOMÍNGUEZ, Ana, *Nuevos retos para la protección de datos personales. En la Era del Big Data y de la computación ubicua*, cit. p. 115

148 GARRIGA DOMÍNGUEZ, Ana, *Nuevos retos para la protección de datos personales. En la Era del Big Data y de la computación ubicua*, cit. p. 116

149 HERNÁNDEZ LÓPEZ, José Miguel: *El Derecho a la Protección de Datos Personales en la Doctrinal del Tribunal Constitucional*, cit., p.29

150 MURILLO DE LA CUEVA, Pablo Lucas y PIÑAR MAÑAS, José Luis: *El derecho a la autodeterminación informativa*, cit., p. 18

vida en sociedad. Uno de los límites a este derecho es la libertad de expresión e información y para su solución, habrá que ver el caso concreto y acudir al principio de proporcionalidad. Otros derechos con los que encuentra limitaciones el derecho a la protección de datos, es con la libertad religiosa y la libertad sindical.[151]

El derecho a la protección de datos es un derecho fundamental con una doble dimensión: una subjetiva (límites a la actividad de los poderes públicos) y otra objetiva (actividad positiva por parte de los poderes públicos).[152]

El concepto del derecho a la protección de datos está ligado al concepto de anonimización y disociación.[153] En muchas ocasiones se llevan a cabo métodos de anonimización de los datos personales para que las empresas puedan publicarlas sin exponerse a infringir la ley de protección de datos personales, por lo que el uso de datos anonimizados es fomentado e incentivado debido a su mejor protección de los datos personales y de la privacidad.[154] Por todo esto, una vez que un set de datos ha sido anonimizado y los individuos no son identificables, la normativa de protección de datos no se aplicaría. Pero los avances del *big data* han hecho que los sistemas de anonimización de datos no sean del todo eficaces, que se pongan en peligro los Derechos Fundamentales de protección de datos y privacidad; además de poner limitaciones al consentimiento. Incluso hace posible que la reidentificación de los sujetos sea más sencilla.[155] Para la mejor gestión de la protección de datos y la anonimización, existe un código de prácticas de ICO (Information Comissioner's Office), en el que se proporcionan consejos de buenas prácticas que serán relevantes para todas las organizaciones que necesitan convertir los datos personales en una forma en la que los individuos no sean identificables.[156] Como vemos la reidentificación supone un grave riesgo a la protección de nuestros datos personales, pero según la Opinión del

151 HERNÁNDEZ LÓPEZ, José Miguel: *El Derecho a la Protección de Datos Personales en la Doctrinal del Tribunal Constitucional*, cit., pp. 59 a 67

152 HERNÁNDEZ LÓPEZ, José Miguel: *El Derecho a la Protección de Datos Personales en la Doctrinal del Tribunal Constitucional*, cit., p. 34

153 ÁLVAREZ, Cecilia: *El poder del usuario digital*, en A. RALLO y R. MAHAMUT (dir), cit, p.292

154 HERNÁNDEZ LÓPEZ, José Miguel: *El Derecho a la Protección de Datos Personales en la Doctrinal del Tribunal Constitucional*, cit., p. 57

155GIL, Elena, *Big data, privacidad y protección de datos,* cit. pp. 83 y ss.

156ICO: «Anonymisation: managing data protection risk code of practice*», cit*.

Grupo de Trabajo del artículo 29[157], se puede saber si una base de datos es anónima o no verificando que el fichero no tenga las propiedades de singularización, asociación e inferencia, y realizando un análisis sobre el riesgo de reidentificación de los datos.[158]

Con todo esto, hay que tener en cuenta que la anonimización puede permitirnos hacer que la información derivada de los datos personales esté disponible en un formulario que es rico y utilizable, al tiempo que protege a los sujetos[159] hasta su posible reidentificación.

En los considerandos 28, 29 y 30 del RGPD nos encontramos con una alusión a la seudonimización ya la identificación de las personas, donde se indica que este sistema puede reducir el riesgo para los afectados y puede permitir a los encargados del tratamiento de los datos cumplir sus obligaciones de protección de datos. Y la identificación de las personas físicas puede realizarse mediante la huella digital que éstas dejan en su interacción con las TIC.

Los métodos más extendidos de seudonimización son la encriptación y la tokenización; aunque en la actualidad, la seudonimización, ya no se considera un método de anonimización, ya que el individuo todavía es identificable.[160] En cuanto a las técnicas de anonimización, nos encontramos con la randomización y con la generalización.[161] Según el Grupo de Trabajo del art. 29[162], determina dos métodos para comprobar si un fichero es anónimo: realizar un análisis sobre el riesgo de reidentificación de los datos, y verificar

157 El Grupo de Trabajo del Artículo 29 fue creado por la Directiva 95/46/CE, es un órgano consultivo independiente integrado por las Autoridades de Protección de Datos de todos los Estados miembros, el Supervisor Europeo de Protección de Datos y la Comisión Europea.

158 GIL, Elena, *Big data, privacidad y protección de datos, cit. p. 109*

159 ICO: «Anonymisation: managing data protection risk code of practice*», cit*.

160 La encriptación: con una clave secreta permite que el dueño de la clave reidentifique a los sujetos desencriptando la clave. La tokenización se aplica al sector financiero para el procesamiento de tarjetas de crédito. La creación del identificador (token), consiste en sustituir los números de DNI por valores de escasa utilidad. GIL, Elena, *Big data, privacidad y protección de datos, cit. pp.89 y 90*

161 La randomización altera la veracidad de los datos con el objetivo de eliminar la asociación entre los datos y el individuo; bien mediante la adición de ruido (modificar los datos de forma que sean menos precisos) o bien por la permutación (intercambiar los atributos de los individuos); y la generalización se refiere a generalizar o diluir los atributos de los sujetos, modificando su escala. GIL, Elena, *Big data, privacidad y protección de datos, cit. p.105*

162 Opinion 05/2014 on Anonymisation Techniques: *http://collections.internetmemory.org/haeu/20171122154227/http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf*

que el fichero no tenga ninguna de las siguientes propiedades: capacidad de singularizar a un individuo, capacidad de asociar, al menos, dos datos pertenecientes a un mismo sujeto; y capacidad de inferir nuevos datos sobre individuos.[163]

4.5. La elaboración de perfiles a través del *big data*

Como hemos hecho referencia a lo largo de este trabajo, una de las principales aplicaciones de los macrodatos es la elaboración de perfiles con la gran cantidad de los datos recopilados gracias a nuestra huella digital, y esta elaboración de un perfil es un tratamiento automatizado de nuestros datos personales. La elaboración de perfiles se contempla en el art. 22 RGPD, donde se introducen nuevas disposiciones sobre el derecho del interesado de no estar sometido estas decisiones automatizadas cuando le produzca efectos jurídicos o le produzca un perjuicio. Esta elaboración de perfiles se utiliza para *"analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona"*.

Los avances en la tecnología, la capacidad de análisis del *big data y* la inteligencia artificial han hecho que cada vez sea más fácil la creación de perfiles provocando un impacto significativo en los derechos y libertades de las personas, ya que, como indica el GT29 en el Dictamen WP251[164], los interesados pueden no saber realmente que están siendo objeto de esta elaboración de perfiles, llevándose a cabo mediante unos procesos poco claros y opacos y en muchas ocasiones sin el consentimiento expreso de los interesados de estos datos. Este análisis de los perfiles que puede suponer un aspecto negativo para los interesados, tiene muchas aplicaciones en el ámbito empresarial. Por consiguiente, entendemos que la recopilación de información sobre las personas permite analizar multitud de características y circunstancias sobre ésta para colocarlos en una categoría determinada y con esto hacer predicciones o evaluaciones sobre sus intereses, gustos o comportamiento.

163 GIL, Elena, *Big data, privacidad y protección de datos, cit. p. 95*

164 GT29, *Dictamen sobre la toma de decisiones individuales automatizadas y la elaboración de perfiles (WP251) del Grupo de Trabajo del Artículo 29,* que podemos encontrar en *http:// ec.europa.eu/newsroom/document.cfm?doc_id=47742*

5. CONCLUSIONES

Después de la redacción de este trabajo hemos llegado a diferentes conclusiones y reflexiones.

1. Hemos podido comprobar que hoy en día, la moneda de cambio es la información, como ya predijo en 1597, Sir Francis Bacon cuando dijo que: *"El conocimiento es poder"*. La consideración que tenemos de que un servicio es gratuito, muchas veces entraña el secreto de que realmente el coste son nuestros datos personales o privacidad sin que tengamos conocimiento de ello.

2. Hemos observado la gran importancia de una regulación en materia de protección de datos unificada en todos los Estados miembros de la UE, ya que cada vez el "Internet de las cosas" es más grande y se cruzan todo tipo de fronteras. Internet no conoce de fronteras y la legislación debe tener en cuenta este aspecto e intentar ir por delante para unirse al resto de Estados, respetando el principio de seguridad jurídica.

3. Consideramos que el nuevo derecho al olvido es un gran avance que permite a los interesados defenderse de las injerencias en sus datos personales.

4. En la realización de este trabajo hemos comprobado la gran evolución que se realiza día a día en las TIC, haciendo prácticamente imposible la tarea legislativa para que pueda ir pareja a estos avances y cubrir todos los aspectos novedosos que van surgiendo.

5. Conociendo el *big data*, hemos aprendido que es una herramienta muy útil para el nuevo modelo de las empresas, donde se intenta estudiar cada paso que da el consumidor para poder ofrecer los mejores productos. Este aspecto que es muy positivo para las empresas, pone en tela de juicio hasta qué punto los interesados estamos dispuestos a este seguimiento y monitorización, exponiendo nuestros datos más personales y desdibujando la diferencia entre vida privada, pública e intimidad.

6. Hemos verificado que existe una gran amplitud de legislación para la protección de nuestros datos personales, de manera general y en ámbitos más específicos, que nos permiten acudir a ella cada vez que lo necesitemos. Y que nos encontramos en un momento de cambio con la entrada en vigor del nuevo

RGPD. Esta legislación se refuerza con la figura de la AEPD, que sirve de apoyo a todos los individuos que necesiten información, consejo e incluso donde se puede acudir cuando hemos sufrido alguna lesión en nuestro derecho a la protección de datos.

7. El nuevo RGPD, que ha empezado a aplicarse este año, ha sido muy esperado desde la última Directiva de 1995, debido a que la evolución que se ha producido desde entonces y la gran cantidad de conceptos tecnológicos nuevos no encontraban una regulación clara y unificada. Estos "vacíos" legales se han intentado remediar con los dictámenes y escritos que publicaba el Grupo de Trabajo del art. 29, que aunque no son vinculantes, han servido para seguir unas guías de comportamiento y de aplicación de algunos aspectos.

8. Hemos analizado el gran debate que existe en cuanto al consentimiento, ya que en muchas ocasiones cuando se otorga, se hace sin saber realmente el alcance de ese consentimiento o incluso sin entender sobre qué se está otorgando ese consentimiento debido al lenguaje farragoso de las políticas de privacidad de motores de búsqueda, redes sociales, etc. Este lenguaje se pide que sea más claro en el RGPD.

9. Hemos descubierto el sistema de anonimización que emplean muchos responsables o encargados de tratamiento de datos para intentar cumplir con la normativa de protección de datos y no violar los datos personales de los interesados. Sin embargo, con el gran avance tecnológico que tenemos hoy en día, la completa anonimización no es posible, ya que se dispone de la tecnología necesaria para combinar gran cantidad de bases de datos y hacer que esos datos anónimos, vuelvan a ser identificados.

10. Hoy en día hay innumerables tecnologías que ponen en peligro nuestros datos personales, por lo que es importante que todos tengamos un gran conocimiento del alcance de éstas cuando las utilicemos. En consecuencia, consideramos que es importante una buena educación en las TIC y en tener en consideración nuestros datos personales, ya que son los datos que nos diferencian y que nos hacen ser nosotros mismos, son nuestra identidad y, como tal, hay que protegerlos.

6. BIBLIOGRAFÍA

CRAIG, Terence y LUDLOFF, Mary E.: *Privacy and Big Data*, O'Really, Sebastopol (California), 2011.

DRUMMOND, Víctor y traducción de ESPÍN ALBA, Isabel: *Derecho de las nuevas tecnologías*, Reus, Madrid, 2004

GARRIGA DOMÍNGUEZ, Ana: *Nuevos retos para la protección de datos personales. En la Era del Big Data y de la computación ubicua*, .ed Dykinson, Madrid, 2015.

GIL, Elena: *Big data, privacidad y protección de datos,* Agencia Española de Protección de Datos, Agencia Estatal Boletón Oficial del Estado, Madrid, 2016. Accésit en el Premio de Investigación de 2015.

GRUPO DE TRABAJO del artículo 29: Recomendación 97/3, sobre el *"anonimato en Internet",* 3 de diciembre de 1997.

GRUPO DE TRABAJO del artículo 29: *"Opinión 05/2014 on Anonymisation techniques"*, 2014.

HERNÁNDEZ LÓPEZ, José Miguel: *El Derecho a la Protección de Datos Personales en la Doctrinal del Tribunal Constitucional*, Thomson-Reuters Aranzadi, Navarra, 2013.

MURILLO DE LA CUEVA, Pablo Lucas y PIÑAR MAÑAS, José Luis: *El derecho a la autodeterminación informativa*, Fundación Coloquio jurídico europeo, Madrid, 2009

NOAIN SÁNCHEZ, Amaya: *La protección de la intimidad y vida privada en Internet la integridad contextual y los flujos de información en las redes sociales (2004-2014)*, Agencia Española de Protección de Datos, Agencia Estatal Boletín Oficial del estado, Premio Protección de Datos Personales de Investigación 2015. Madrid, 2016

RALLO, Artemi: *El derecho al olvido en Internet: Google versus España*, Centro de Estudios Políticos y Constitucionales, Madrid, 2014

RALLO, Artemi y MAHAMUT, Rosario: *Hacia un nuevo derecho europeo de protección de datos*, Tirant lo Blanch, Valencia, 2015

REBOLLO DELGADO, Lucrecio: *El derecho fundamental a la intimidad*, 2ª ed., Dykinson, Madrid, 2005

TERCEIRO, José B.: *Socied@d digit@l. Del homo sapiens al homo digitalis*, Alianza Editorial, Madrid, 1996.

TERCEIRO, José B. y MATÍAS, Gustavo: *Digitalismo: el nuevo horizonte sociocultural*, Grupo Santillana de Ediciones, Madrid, 2001

VALLS, Josep-Francesc: *BIG DATA: atrapando al consumidor*, Profit editorial, Barcelona, 2017

7. ANEXOS

7.1. Páginas web

ACXIOM: *https://www.acxiom.com/what-we-do/*

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD): *Guía del Derecho Fundamental a la Protección de Datos de Carácter Personal*, 2004. *https://www.agpd.es/portalwebAGPD/common/FOLLETO.pdf*

AEPD: funciones *http://www.agpd.es/portalwebAGPD/LaAgencia/informacion_institucional/conoce/funciones-ides-idphp.php*

AEPD: guía del Reglamento de Protección de Datos para responsables de tratamiento: *http://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/guia_rgpd.pdf#Gu%C3%Ada%20del%20Reglamento%20General%20de%20Protecci%C3%B3n%20de%20Datos%20para%20responsables%20de%20tratamiento*

AEPD, información sobre el Grupo de Trabajo del Artículo 29: *http://www.agpd.es/portalwebAGPD/internacional/Europa/grupo_29_*europeo/index-ides-idphp.php

AEPD: Registro General de Protección de Datos: *https://www.agpd.es/portalwebAGPD/canalresponsable/inscripcion_ficheros/index-ides-idphp.php*

AEPD: Reglamento de Protección de Datos: *http://www.agpd.es/portalwebAGPD/temas/reglamento/index-ides-idphp.php*

BOE corrección errores RGPD*: http://www.boe.es/buscar/doc.php?id=DOUE-L-2018-80845*

BOE enmiendas RGPD: *http://www.congreso.es/public_oficiales/L12/CONG/BOCG/A/BOCG-12-A-13-2.PDF*

ELDERECHO.COM: *http://tecnologia.elderecho.com/tecnologia/privacidad/tramitacion-LOPD-Congreso-proteccion-datos_11_1197055003.html*

EL ECONOMISTA:
http://www.eleconomista.es/legislacion/noticias/9060579/04/18/El-Supremo-rechaza-conceder-el-derecho-al-olvido-a-personas-publicas.html
EMPRESITE: *http://empresite.eleconomista.es/GOOGLE-SPAIN.html*
FUNDACIÓN HUMANA PRO DERECHOS HUMANOS:
http://www.derechoshumanos.net/constitucion/articulo18CE.htm
GENBETA: https://www.genbeta.com/actualidad/microsoft-quiere-impedir-que-las-autoridades-de-estados-unidos-accedan-a-datos-que-almacenan-en-otros-paises
GRUPO DE TRABAJO ART. 29:
http://collections.internetmemory.org/haeu/20171122154227/http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf
GRUPO DE TRABAJO ART. 29: Dictamen sobre la toma de decisiones individuales automatizadas y la elaboración de perfiles (WP251):
http://ec.europa.eu/newsroom/document.cfm?doc_id=47742
GTI: *http://www.gti.es/es-es/Nextwave/Paginas/BigData/big-data-concepto.aspx*
ICO: https://ico.org.uk/media/1061/anonymisation-code.pdf
OSI: *https://www.osi.es/es*
SERFINASA: http://www.serfinansa.com.co/servicioclientе/leyhabeasdata
Sinopsis artículo 18 de la Constitución Española:
http://www.congreso.es/consti/constitucion/indice/sinopsis/sinopsis.jsp?art=18&tipo=2
USERVERS: *http://web.uservers.net/ayuda/soluciones/dominios/que-es-una-direccion-ip_NTk.html*
WIKIPEDIA GOOGLE: *https://es.wikipedia.org/wiki/Google*

7.2. Sentencias consultadas

- Sentencia 290/2000, de 30 de noviembre de 2000 del Tribunal Constituciona.

- Sentencia 292/2000, de 30 de noviembre de 2000 del Tribunal Constitucional.

- Sentencia 6/11/2003, del Tribunal de Justicia de la Unión Europea (TJUE), caso Lindqvist.

- Sentencia de 24 de noviembre de 2011 del Tribunal de Justicia de la UE.

- Auto de 27 de febrero de 2012, de la Audiencia Nacional (RJCA 2012/321).

- Sentencia de 8 de febrero de 2012, del Tribunal Supremo (RJ 2012/291).

- Sentencia del Tribunal Constitucional 17/2013, de 31 de enero.

- Sentencia de 8 de abril del 2014 del Tribunal de Justicia de la UE (C-293/12)

- Sentencia 13 de mayo de 2014 del Tribunal de Justicia de la Unión Europea.

- Sentencia de 29 de diciembre de 2014 de la Audiencia Nacional (RJCA 2014/1065).

- Sentencia 1611/2016 de 4 de julio del Tribunal Supremo (AEPD vs Google).

8. SUMMARY IN ENGLISH

Nowadays technology constantly surrounds us in all the activities we do. All the interactions we have with the technologies are registered and all this information, added to the rest of the people in the world, is what is called big data. Big data is also called the technologies that are used to treat this large amount of information. That interaction of ours is what defines us in the digital world and is the fingerprint.

The vast majority of this information we give ourselves for free, either to enter a social network or to make an online purchase. The problem is that many times we are not aware of the great scope that can have expose our data in this way. Another part of the information that is stored, is that which is obtained without us noticing, through the use of cookies or other applications that are installed on our devices, many times without our consent.

While the information is retained in the devices, there is no violation of our privacy, the violation exists when this information leaves our computer and ends up in the big servers of the information managers. These data managers are those who store and treat them, and, in many cases, transfer them to third-party companies for use with different purposes. One of these purposes, may be its use for advertising. Many times we see that after having been looking for something in our Google browser, we see ads on Facebook or other pages that we enter, referring to that search we have previously done and this is thanks to the big data technologies. Each user can be identified through his computer profile.

All the technological and computer change that has occurred during all this time has also produced a change of mentality in the people who interact with this technology, since we relate in a very different way to how it was done before the great revolution of the technologies. The change from Web 1.0 to Web 2.0 has meant that the interaction is more active and that we exchange information with each other practically immediately and often without taking into account the consequences of this interaction for the protection of our data.

The application of big data technologies have many advantages and disadvantages for people and companies. On the one hand, as advantages we

find that big data has allowed these technologies to be used to help develop new concepts of commerce with personalized advertising, and may also reach a greater number of people and people who, according to their digital profile, They are more willing to buy those products. These techniques, together with data mining, have been and continue to be used by companies to also develop new products on the needs of individuals. It has also been possible to create online advertising that allows each person to offer a series of different advertising based on their interests and tastes (thanks to cookies and other types of technologies) and to make decisions more quickly and efficiently. The advantages it brings to users are instant communication with everyone and a very complete and predictive web browsing experience.

On the other hand as disadvantages to these big data technologies we find the great sacrifice we make to obtain all of the above, which is to endanger our privacy and our personal data with the intrusion in our private life that this entails. There is a risk of applying this technology to all without human intervention and that the decisions end up being artificial and without finally having a revision by the people, making that, in many occasions, these decisions or conclusions are not correct. This may be because the big data has the ability to relate thousands of data that combined seem to have some meaning, but that really is not so. The new technological world is very broad and global and without realizing it we can share information with people we do not really know and who can use this information for very different purposes and harmful to us.

The large amount of information available to companies entails a serious risk in their storage, treatment and subsequent use. However, the problem of putting our privacy at risk increases with the rest of the technologies that we have available to us every day and that we do not realize to what extent it harms our privacy. These technologies are found in smartphones, activity wristbands, computers, geolocation devices, monitoring technology and RFID tags. These devices and technologies help to gather information to be later treated with the data mining that creates the technological profiles.

Having all this information, the data providers are those who benefit from this data, who process and perform analysis and then make available to the different companies and organizations that may be interested in having this information of their potential customers.

When we talking about big data, we have to take into account other concepts, such as consent, the right to data protection, privacy and privacy. In consent is a very important aspect to consider when we talk about collecting and treating someone's personal data. The consent of the affected person is needed in order to obtain this data and for its treatment, the problem arrives at the moment of using this data, since many times, when these data are collected, the potential that they have is unknown. and it is not known what they will be used for finally. This leads to the servers that obtain this information have to request consent for each use they want to give, however, not always done so.

The fundamental right to data protection has ended up becoming a third generation autonomous fundamental right, which has derived from the right to privacy of articles 18.1 and 18.4 of the Spanish Constitution of 1978. Personal data, according to article 4 RGPD, all the information about an individual that is identifiable and that are specific to their identity. So the right to data protection entails that any individual who sees their personal data in danger or violated, can exercise this right to perform all actions necessary to protect them. For the help of this data protection we find the Spanish Data Protection Agency (AEPD) at the national level and the European Data Protection Supervisor (EDPS), to ensure the treatment of personal data in the institutions of the European Union . These two bodies are independent and are responsible for collecting the complaints we have about the protection of our personal data, as well as advising companies on the correct treatment of the data they carry out in their functions.

When we talk about the protection of personal data, we have to talk about the anonymization system, through which the necessary mechanisms are made so that the owners of these personal data are not identifiable. With this system companies can avoid violating data protection laws, since, as people

are not identifiable, the data protection law would not be applicable. However, anonymization techniques run the risk of the application of big data technologies, since they allow the reidentification of this information by combining a large amount of information to be able to identify the individuals who own these data.

The right to privacy is a fundamental right that is often confused with privacy in our system. However, we must bear in mind that private life contains information that we do not want to be known, and privacy is something that is within that private life and that we protect with greater intensity, because it contains aspects that nobody knows about us.

All these concepts are collected, protected and regulated by different national and European laws. Our Constitution includes the fundamental rights to the protection of personal data on the Internet, privacy and honor, among others; providing them with an organic law reservation of their article 81.

At the European level we find Directive 95/46/EC, of 24 October, on the protection of natural persons with regard to the processing of personal data and the free circulation of these data. This Directive, until the establishment of the new General Data Protection Regulation 2016/679, of 27 April (GDPR), has been the reference text on the protection of personal data. Directive 95/46 set limits on the collection and use of personal data, in addition to determining the creation of independent national bodies to supervise the processing of these data and their protection, as is the case of the AEPD in Spain. This Directive regulates the ARCO rights, (access, rectification, cancellation and opposition) and the right to information.

This Directive 95/46 was transposed by Spain through the Organic Law 15/1999, of 13 December, on the Protection of Personal Data (LOPD) and the regulation that develops it, approved by Royal Decree 1720/2007, of 21 December (RLOPD). The LOPD bears many similarities with the regulation made in Directive 95/46. Because the fundamental right to data protection is only enforceable by natural persons, both Directive 95/46 and the LOPD will only apply to natural persons. The LOPD recognizes the rights ARCO (arts. 15, 16 and 6.4 LOPD), the rights to challenge (art. 13 LOPD), compensation (art. 19

LOPD) and consultation of the General Data Protection Register (art. 14) LOPD). Another aspect that deals with the LOPD is the automated decision making of art. 13.1 LOPD, aspect that refers to the use of big data technologies to make decisions without human intervention.

The LOPD specifies that the consent granted for the processing of personal data must be unambiguous and can only be revoked when there are justified causes (art. 6 LOPD).

This work could not miss the reference to the GDPR that came into force on May 25, 2016 and that was applied on May 25, 2018, repealing Directive 95/46. The LOPD remains in force until a new national data protection law is made, but it will only be applied in what does not oppose the GDPR. There was a great need to renew Directive 95/46 because of the great technological advances that had taken place since then and that did not contemplate the Directive. This Regulation seeks legislative unification in all EU countries, since this Regulation is directly applicable in the member countries and a transposition to national legislation is not necessary, so it will help all member states to apply equally. legislation and there is greater legal security throughout the European territory for the protection of the rights of individuals.

The GDPR adds many new features, such as:

- The territorial scope: it is established that this regulation will be applicable throughout the European territory and for all companies, even if they do not have an establishment in Europe, if they direct their offers to the citizens of the EU. Very important point, since there has always been a great debate about what a person could do when their right to data protection was violated by companies or organizations that do not have their headquarters in a European country, like Google or Facebook.

- The consent becomes explicit in the sense that the request for this consent must be made in a clear and easily understood manner. In addition, it establishes the age of children under 16, requesting for these, the consent of their parents or guardians.

- They have added in the part of personal data of special protection: the treatment of genetic data and biometric data.

- The principles of legality, loyalty and transparency are incorporated (art. 5 GDPR), privacy from the design and by default (art. 25 GDPR), and quality.

- The right to be forgotten (art. 17 GDPR): a right that, despite being collected before in a Spanish sentence, had not been regulated. The right to be forgotten allows the individual to request that information be removed or deleted from the Internet and that all necessary means be carried out so that this information is not returned to the Internet. This right can be exercised as long as it does not conflict with the right to information or the right to freedom of expression, since the principle of proportionality must be applied to consider which right is above the other in each specific case. In addition, in a very recent judgment of the Supreme Court of April 4, 2018, in which the right to oblivion is limited to the data of public figures.

- Other rights: right to limitation of treatment (art. 18 GDPR) and to the portability of the data. The limitation of the treatment refers to the future treatment that can be done of the obtained data, that is, to be able to control that treatment as long as a series of conditions are met. The portability of the data refers to the right that an individual has to carry their data from one server to another.

- Automated decision-making and creation of profiles (art. 22 GDPR): as we have indicated before, automated decision-making is prohibited as long as it affects the individual legally, but in our day to day we find that this automated decision making is used in many aspects, such as when deciding if we are granted a loan. Profiling is the automated treatment that is carried out using a set of personal data to try to predict what behavior or needs you will have.

- Protection of data by default and from the design (art. 25 GDPR): the protection from the design is that the company carries out the necessary measures to ensure data protection and privacy in the processing of this data from the moment in which they are collected. The default protection would be that by default a company will guarantee all the necessary rights for the protection of the data and that they are not accessible to an undetermined number of people.

- It is urged that there is a cooperation between the different independent data protection agencies of each member country (art. 31 GDPR).

- A key element of this Regulation is the creation of the figure of the Delegate for Data Protection (DPO) (arts. 37 et seq.). This DPO will act independently and is a guarantor of the data protection regulations in organizations that carry out data processing as a main activity and for authorities and public organisms.

- The competent data protection authority must be notified of the data security breaches that occur in the companies within a period of no more than 72 hours after the data controller has been certified (art. 33 GDPR).

- It also reinforces the treatment of data transfers to third countries in arts. 44 et seq. GDPR, establishing some limits and guidelines to follow for its correct execution.

With all these modifications we can see how necessary this GDPR was to adapt the legislation to the great technological advances that we have observed over time.

Another Directive that we have taken into account in this work is Directive 2006/24/EC of the European Parliament and of the Council, of March 15, of Retention of Data, that although it is repealed, the law that transposed it to our order, the Law 25/2007, remains in force. This Law allows operators that provide electronic communications services or exploit public communications networks, keep the data of these communications for a minimum period of 6 months and a maximum of 2 years, which can be delivered to the corresponding agents and prior judicial authorization (arts. 5 and 6 Law 25/2007).

When we talk about legislation it is important that we take into account that information on the Internet crosses borders constantly and without us noticing. This has to be taken into account when we want to apply a specific legislation, since we can have problems to determine which territory should apply its laws. If the problem with data protection is between European countries there would be no problem, since European legislation has been unified with the entry into force of the GDPR. However, when we speak of third

countries, it is more complicated, because the legislation can vary. For example, in the USA National security goes beyond any protection of individual personal data, and this was reinforced after the 9/11 attack and all those who have suffered. This supremacy of security causes that in these countries there are many violations of privacy and data protection of citizens, making a control over them and even about the European institutions. With the GDPR and its territorial application it is tried that these barriers are demolished when applying the European Regulation to the entities that realize publicity in European countries.

With such a technological society before us, it is important that both citizens and companies and organizations have clear rights and obligations in the protection of personal data. Individuals are those who historically have been most unprotected against the companies and organizations that treated their personal data, however, with the new legislation, it wants to impose certain obligations on companies so that this situation does not happen again. Taking into account all of the above, we can see that citizens are endowed with a series of rights that they can exercise at any time to protect their personal data and their privacy before the courts that are competent.

Organizations and companies that carry out some type of personal data processing must take into account all the guarantees they have to ensure not to violate the new Regulation and, above all, take into account the anonymization or pseudonymization that the GDPR contemplates, in addition to the figure of the DPO to supervise the correct application of the Regulation.

In this project we have emphasized the importance of consent in the processing of personal data, since not request the consent of the data subject for the collection and processing of data, these data would be considered to have been collected illegally. In the collection of consent by the person responsible for the processing of personal data, some requirements must be followed in order for this consent to be valid. The consent must be free and express and the person responsible for the treatment must have complied with the requirement that the information given to obtain the consent has been written in a simple way and with a simple language so that it can be understood

by all citizen. The burden of proving that the consent has been granted correctly is the responsibility of the treatment. To all this we must add that the consent can be withdrawn at any time and must be able to be carried out in a simple way as well. We must bear in mind that, in many occasions, we give our consent even without reading the damages that this may have for our personal data. This sloppiness is not simply for not wanting to read, but because on many occasions, if not always, the data protection policies of social networks or search engines are very extensive, confusing and written in such a way that only an expert in Data protection could decipher. This aspect is the one that wants to change the GDPR when it talks about that when informing the consent it must be done in a clear way and with simple language.

To conclude, we consider that the application made by social networks of data protection legislation is of special interest, because, although we have not been able to approach in this work, we interact in them exchanging a lot of information thinking that we only do it with our closest circle.