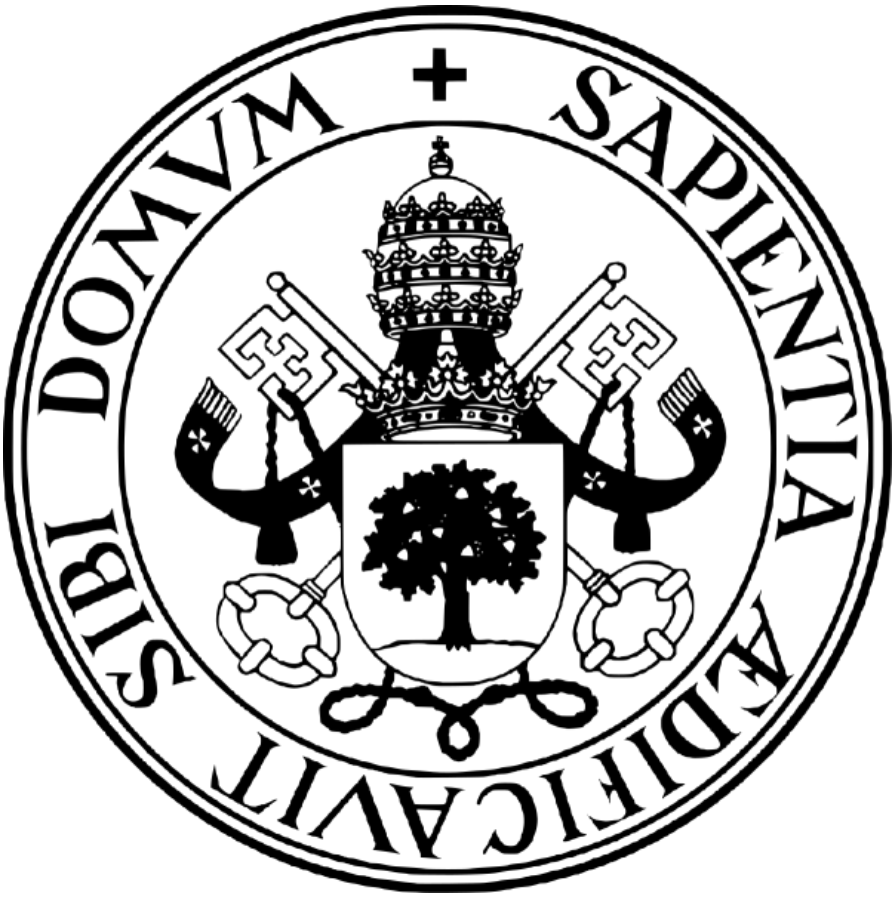

FACULTAD DE CC. Sociales, Jurídicas y de la Comunicación

UNIVERSIDAD DE VALLADOLID

Grado en Derecho

BIG DATA

Autor: Mario Moreno Garcinuño

Curso 2019/2020

TUTOR: Carmen Herrero Suárez

Resumen: El presente trabajo abarca el análisis del concepto *Big Data*. El objetivo de este trabajo es analizar desde una perspectiva jurídica la incidencia de la tecnología y los macro datos en los distintos ámbitos. Se analizará la influencia de este concepto en los derechos y libertades tradicionales, así como el desarrollo normativo que encontramos hasta la fecha. Por otra parte, se valorará la introducción de esta tecnología en otros ámbitos, así como la necesidad de desarrollar y extender la normativa a estos nuevos ámbitos.

Palabra claves: Big Data, macro datos, derechos fundamentales, desarrollo normativo, riesgos tecnológicos

Abstract: This work studies the analysis of the *Big Data* concept. The objective of this work is to analyse the incidence of technology and "macrodata" in the different areas from a legal view. The object of this work is to assess the incidence of this concept on traditional rights and freedoms, as well as the normative development until the date. Furthermore, the technological inclusion in other areas will be studied, as well as the development and growth of the regulations in new areas.

Key words: Big data, macrodata, fundamental rights, normative development, technological risk

INDICE

1.- INTRODUCCIÓN: EL "*BIG DATA*" CONCEPTO Y CARACTERES

Este trabajo tiene sentido en nuestra sociedad actual debido a los grandes avances tecnológicos que hemos ido sufriendo a lo largo del tiempo, especialmente desde la aparición de Internet. Internet viene a dar pie a una nueva forma de entender el mundo y produce un sinfín de conceptos novedosos, supone la creación de un "mundo" dentro de nuestro mundo, en el cual todo está al alcance de nuestra mano con muchas facilidades, lo que comporta, indudablemente, innumerables efectos positivos, pero también puede entrañar ciertos riesgos.

En este marco temporal nos encontramos con el término "*Big Data*" que viene a explicarse de una forma sencilla como "grandes cantidades de información". Esta información es almacenada gracias en gran parte a la conexión que brinda Internet, que facilita el movimiento de datos, también se apoya en otras tecnologías para no solo almacenar esta información si no realizar un procesamiento de esta información para que a través de esa interpretación de los datos la información resulte útil para los objetivos que se marquen.

Esto se traduce en un ejemplo práctico, desde la perspectiva de las empresas, estas habrán de trabajar y potenciar tanto la recopilación de datos como el procesamiento de la información para poder ser más competitivas. Las empresas emplearan el *Big Data* para guiar, a través de sistemas de trabajo más eficientes y actualizados, sus campañas de marketing y también conocer a sus usuarios, así como la situación del mercado. El conocimiento que brinda la información procesada servirá para poder iniciar conductas que beneficien la interactuación con los usuarios y también para llegar a otros que no se sienten atraídos por la actividad de la empresa.

Esta información puede obtenerse de forma directa a través de la aceptación de recogida de esos datos, pero, en otros casos, el *Big Data* puede emplearse para procesar de tal forma la información que se elaboren perfiles y se genere información sobre nuestro comportamiento y preferencias. Cabe mencionar en este punto que no siempre la captación de la información puede provenir de una empresa privada ya que las administraciones publicas también emplean el *Big Data* para potenciar su rendimiento.

Quiero mencionar brevemente que en este trabajo se abordará tanto la responsabilidad que tienen las empresas en la captación como en la protección de datos. Es

evidente que a través de la captación de datos pueden verse comprometidos los intereses de los usuarios y en ocasiones los "derechos digitales", las irregularidades en la captación pueden llegar a suponer una injerencia, por ejemplo, en los derechos fundamentales, concretamente a los que tratan la protección de la intimidad. Además, el grado de diligencia que se exige a las empresas no queda solo en la captación de la información, sino que se extiende a la protección de los datos, fundamentado, sin duda, en la cantidad y el valor de la información recopilada, que de caer en malas manos supondría un riesgo viendo los derechos de los usuarios comprometidos y la actividad de la empresa puesta en duda. Estas situaciones, junto a la escasa regulación existente hasta el momento, hacen que muchos derechos y libertades se vean afectados, y este peligro obliga a establecer un marco de responsabilidad para aquellos que empleen el *Big Data*.

El nacimiento del *Big Data* no está definido temporalmente, en gran parte, debido a la inexistencia de un concepto uniforme sobre este fenómeno, lo que dificulta la identificación de su origen.

Parte de la doctrina que discute los orígenes del *Big Data* encuentra reminiscencias tras la II Guerra Mundial a través de la creación de hardware de memoria que permite el almacenamiento de datos, apareciendo a finales de los años 60 sistemas más avanzados que permitían almacenar datos de una forma automática y rápida.

En 1989 Erik Larson hace una mención que se asemeja a nuestro concepto actual de *Big Data*, aparecen sistemas de análisis de la actividad comercial bajo el término "*business intelligence*" [1] que viene a ser un modo de actuación encaminado a optimizar las actuaciones de las distintas empresas y que viene a ser el concepto que precede al actual *Big Data*. En este momento histórico aparece también la red informática mundial ("*World Wide Web*") entendido como un sistema de distribución de documentos interconectados a través de Internet, lo que brinda una posibilidad inmensa en relación con el flujo de información.

Posteriormente aparecen empresas pioneras como Hortonworks y Cloudera que tratan de aprovechar estos datos, implementando sistemas de gestión de datos, tratando de aprovechar la alta demanda de sistemas para el procesamiento de datos por parte de las diferentes empresas. Y esto ha llegado a la actualidad, donde las empresas para ser realmente competitivas han de desarrollar una fuerte inversión en *Big Data* y "*Machine Learning*" que

[1]NIÑO, M. e ILLARRAMENDI, A.: *"Entendiendo el big data",* disponible en https://www.dyna-newtech.com/busqueda-NT/entendiendo-big-data-antecedentes-origen-y-desarrollo-posterior

viene a analizar la información disponible a través de algoritmos para predecir comportamientos.

El *Big Data* ha tomado tal relevancia que actualmente se emplea en política. Su uso tiene como precedente las elecciones en Estado Unidos, con Barack Obama como candidato se emplearon sistemas para conocer las opiniones de los votantes y con esa información convenientemente procesada elaborar una campaña más optimizada para alcanzar a los votantes más indecisos.

Actualmente y, previsiblemente en el futuro más inmediato, el *Big Data* apunta como un concepto de gran relevancia en casi todos los ámbitos de la vida, esto viene de las facilidades que se plantean actualmente a través del acceso a Internet desde múltiples dispositivos, las mejoras tecnológicas que facilitan el procesamiento de datos y la aparición de empresas especializadas que trabajan en el ámbito del *Big Data* para exprimir al máximo sus posibilidades y potenciar los resultados de su uso.

El "*Big Data*"[2] es considerado como "macro datos" complejos, que tendrán tal consideración cuando excedan la capacidad de captación y procesamiento de los modelos tradicionales. Esto es posible gracias a los avances que brinda la tecnología para emplear nuevas estrategias y arquitecturas para la recopilación y análisis de grandes volúmenes de datos. Las características propias del *Big Data* serán: volumen (gran cantidad), velocidad (en la creación y procesamiento) y variedad (cualquier dato de cualquier fuente puede ser empleado).

Pese a su interpretación literal, el término "*Big Data*" es empleado para referirse al procesamiento de datos, entendido como el análisis de los datos almacenados obteniendo patrones de conducta o tendencias generales, siendo esa información empleada para obtener un rendimiento. La importancia que ha tomado en la actualidad se debe en gran medida a la revolución digital ya que han aparecido técnicas que permiten explotar al máximo el potencial de esta información. Es ahora cuando el "*Big Data*" toma forma aplicando técnicas que emplean inteligencia artificial, modelos predictivos, técnicas estadísticas, etc. Supone un avance abismal respecto a conceptos previos como "*business intelligence*", que, simplemente, localiza información específica dentro de una base de datos, mientras que el "*Big Data*" es capaz de extraer esa información específica e identificar tendencias generales.

[2]JOYANES, L.: "*Big Data, Análisis de grandes volúmenes de datos en organizaciones*", ed. Alfaomega, México, 2013, pp. 19 y ss.

En conclusión, el "*Big Data*" es un concepto novedoso que nace y se confecciona gracias a la revolución digital. El término, literalmente, hace referencia a los "macro datos" aunque su uso se emplea también para referirse al procesamiento de tales datos. Las principales novedades y características del "*Big Data*" son que, en este marco tecnológico, es capaz de captar información de distintas fuentes, con una capacidad de procesamiento y almacenamiento colosal y a una velocidad tal que los medios tradicionales no pueden competir.

Además, conviene señalar que el "*Big Data*" se asienta en la actualidad como un instrumento de gran utilidad en distintos ámbitos. A raíz de la pandemia causada por el COVID-19[3] en determinados países se han desarrollado aplicaciones para el control de sus ciudadanos. En China el gobierno ha lanzado una aplicación que permite controlar los movimientos de la población y la interactuación con otros individuos para aislar a las personas que tengan contacto con un positivo. Esta limitación de los derechos de los ciudadanos permite controlar de manera efectiva los posibles focos de contagios y aislar a la población para evitar la propagación del virus. Esto supone una restricción de la libertad de movimiento y una intromisión en la intimidad de las personas que se justifica con el efectivo control de la pandemia.

Otro de los aspectos novedosos en que se ha empleado el "*Big Data*" es en la obtención de rendimientos económicos a través del procesamiento y uso de datos. Es una realidad que alrededor de los datos se ha creado una industria que es aprovechada por las empresas y por los entes estatales e internacionales. En el marco de la Unión Europea, además de crear un espacio en el que puedan transferirse estos datos, se va a emplear este nuevo mercado de datos para obtener financiación a través de las tasas digitales. Estas tasas vienen a gravar determinadas operaciones digitales en las que se procesan y transfieren datos.

Parece evidente que el Big Data es un instrumento que se encuentra presente en la actualidad y que va a extenderse a todos los ámbitos de nuestra vida junto con la tecnología y, por ello, hay que valorar las repercusiones que tiene el Big Data en el presente y en el futuro para adaptar la normativa estatal y europea a esta nueva realidad.

[3]"Inteligencia artificial y big data contra el coronavirus" disponible en: https://www.lavanguardia.com/tecnologia/20200329/4882486265/cororonavirus-inteligencia-artificial-big-data-drones-robots.html

2.- POSIBLES REPERCUSIONES DEL *BIG DATA* DESDE UNA PERSPECTIVA JURÍDICA

2.1 ¿Cómo afecta a los derechos fundamentales?

Según la doctrina constitucional[4], los derechos subjetivos se diferencian de los derechos fundamentales en que estos últimos han de aparecer recogidos en la Constitución, e intrínsecamente se plantea como necesario que una Constitución, para ser tal, contenga derechos fundamentales. Estos derechos fundamentales son los pilares de los Estados democráticos tal y como se presentan en la actualidad, ya que su introducción supuso el fin del antiguo régimen. Cabe mencionar que, debido a la relevancia que presentan, los derechos fundamentales gozan de una especial protección, tanto el plano estatal como en el plano internacional, lo que se traduce en la posibilidad de acceder a mecanismos de protección de derechos. En este sentido encontramos los recursos ante el Tribunal Constitucional para la protección de los derechos recogidos en el Título I de la Constitución "De los derechos y deberes fundamentales" o el Tribunal Europeo de Derechos Humanos que viene a proteger lo establecido en el Convenio Europeo de Protección de los Derechos Humanos y de las Libertades Fundamentales.

Con el auge del *Big Data* la protección de los derechos fundamentales ha de evolucionar y extenderse. Son los avances tecnológicos los que hacen que la sociedad evolucione, y con ella debe hacerlo también el Derecho, es decir, la técnica legislativa habrá de evolucionar y adaptarse para cubrir los nuevos frentes, todo ello con el fin de garantizar la protección de los derechos fundamentales.

En este sentido, resulta relevante comentar la intención que tenía la *Convención para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal*[5] de 28 de enero de 1981 que planteaba en su artículo 1, como objeto, brindar una protección a los derechos de las personas sin tener en cuenta su nacionalidad o residencia, simplemente brindar una protección efectiva de los derechos y libertades, en concreto "el derecho a la privacidad en relación con el procesamiento de datos que realiza el *Big Data*".

---

[4]PONS, M.: "*La doctrina constitucional de los derechos fundamentales. Evolución histórica*" en LÓPEZ A., GUTIÉRREZ I.: "*Elementos de Derecho público*", ed. Marcial Pons, Madrid, 2002, pp. 96 y ss.

[5]*Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, Estrasburgo, 28 de enero de 1981, disponible en https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108

En el ámbito de la Unión Europea presentan especial relevancia en el plano de los derechos fundamentales, el artículo 16.1 del Tratado de Funcionamiento de la Unión Europea, que establece que "t*oda persona tiene derecho a la protección de los datos de carácter personal que le conciernan*" y el artículo 8.1 de la Carta de los Derechos Fundamentales de la Unión Europea que mantiene la idea de que "*toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan*". Marcando estos artículos la idea de que toda persona tiene derecho a la protección de datos personales.

Respecto a la Constitución Española, el artículo 18, además de garantizar el derecho al honor, intimidad y propia imagen, en el apartado 4 se hace una referencia a que será la ley la que venga a limitar el uso de la "informática" y con ello las diferentes tecnologías que aparezcan, incluido el *Big Data*, para garantizar los derechos de las personas.

La problemática se plantea a la hora de establecer los límites del *Big Data*, y es que, con la gestación de este concepto han aparecido nuevas posibilidades que plantean a su vez grandes riesgos. La injerencia en los derechos fundamentales puede recaer en la obtención o uso de la información y, además, debemos de tener en cuenta tanto la cantidad de información como calidad y sensibilidad de los datos. Parece claro que la vulneración de la intimidad no atiende solo a la cantidad de información, sino que aborda otros factores como el ámbito al que afecte la información, la consideración que cada persona le dé, etc. Por lo tanto, es posible que la vulneración de los datos personales afecte a un único individuo, pero también, al tratar el *Big Data* grandes cantidades de información, pueden resultar afectados multitud de sujetos. Se entiende, que el análisis de esta problemática habrá de recaer sobre el contenido de esta información, valorando desde una perspectiva objetiva que información encuentra resguardo bajo el derecho a la intimidad y a la protección de los datos personales. Además, como es evidente, habrá que atender al uso que se dé al *Big Data* que puede llegar a afectar al derecho a la igualdad y no discriminación.

Parece, por lo tanto, que toda persona tiene derecho a la protección de los datos personales. Algunos de estos datos pertenecen a nuestro ámbito más íntimo, aquel que está protegido por los derechos fundamentales. En este punto se plantea la cuestión relativa a la protección que nos brinda nuestro hogar, la cual se materializa a través de la inviolabilidad del domicilio junto con el derecho a la intimidad personal y familiar. Se forma por tanto una protección que de alguna forma el *Big Data* puede venir a derribar, y es que, a través del acceso por medio de un ordenador, *smartphone*, *tablet*, etc. se abre una brecha en esta

protección ya que de tu propio hogar está saliendo un flujo de información a través de la red que está siendo atrapado y procesado por empresas para su posterior uso.

Todos estos medios de captación de información pueden llevar a situaciones en las que se produce una vulneración de la intimidad, dado que, con el uso de motores de búsqueda o aplicaciones, aceptamos condiciones que pueden suponer el acceso a información personal como nombre, residencia, número de teléfono, etc. hasta determinados accesos a historiales de búsqueda, geolocalización de dispositivos informáticos, etc. Por lo tanto, la recopilación de datos aislados no relativos a nuestra intimidad puede llevar a la obtención, a través del procesamiento, de otra información que puede afectar a un ámbito íntimo. En consecuencia, debemos valorar los riesgos a los que nos exponemos al emplear ciertos servicios gratuitos, y, además, debemos tener en cuenta que el brindar acceso a cierta información puede derivar, mediante el procesamiento, en la obtención de información más detallada que afecte a la intimidad, pudiendo llegar a conocerse nuestras ideas políticas, religiosas e incluso datos relativos a nuestra salud.

Por ello, bajo mi punto de vista se ha creado una forma de vigilancia y control de datos que infiere en la esfera más interna de la persona y que viene a producir injerencias en los derechos fundamentales. Nos resultaría extraño y violento que el dependiente de una tienda indagara en nuestra vida y nos ofreciera el producto que más se ajusta a nuestra circunstancia o necesidad, pero no nos resulta extraño que tras buscar un producto o simplemente mencionarlo aparezcan multitud de anuncios en nuestro ordenador o *smartphone* en relación con el producto que buscamos. Se trata de una forma de acceso a nuestra intimidad que en determinados casos no apreciamos, ya que al no ser conscientes de cómo se obtienen esos datos, no nos incomoda. Es importante comenzar a plantearse tanto la cantidad como sensibilidad de la información que cedemos al realizar compras online, utilizar redes sociales, realizar búsquedas online, etc. ya que el asunto no acaba en la simple captación. La cuestión alcanza también el uso que se dé a esos datos, pudiendo llegar a ser empleados con fines fraudulentos que perjudiquen a las personas. Por ello, debemos de prestar atención y tener en cuenta que el uso de la tecnología no puede hacerse sin tomar precauciones y siempre teniendo en cuenta que la tecnología también puede vulnerar nuestros derechos.

A través de la exposición en redes sociales, nuestro ámbito de intimidad también se ha visto reducido, y es que el *Big Data* abarca todos nuestros datos y esto se traduce en una vigilancia constante y muy eficaz de las personas.

Un claro ejemplo del control que se ejerce sobre las personas y que incide de manera clara en nuestras libertades también se aprecia en la información recopilada a través de la geolocalización, con la intención de brindar una mejor experiencia a los consumidores, ciertas empresas emplean a través de diferentes medios la información sobre la ubicación de sus clientes para potenciar la publicidad. Esta vigilancia supone un control tal que nuestra intimidad se ve comprometida en un alto espectro.

También pueden plantearse problemas desde una perspectiva jurídica en relación con el principio de igualdad recogido en el artículo 14 de la Constitución Española que viene a consagrar la igualdad ante la ley y la no discriminación. El uso del *Big Data* puede resultar discriminatorio en el ámbito laboral ya que puede ejecutarse la contratación y selección de personal a través de la elaboración de perfiles que marquen la toma de decisiones a la hora de contratar o promocionar a determinados trabajadores. Esto quiere decir, que ante un supuesto de contratación entre dos personas resulta decisiva la elaboración del perfil, que afectará de forma positiva o negativa a las personas según la información que hayan vertido a través de la red, pudiendo en determinados casos resultar un lastre que impida a las personas acceder a ciertos trabajos.

Se plantea otra problemática respecto a la discriminación, pudiendo ser económica o social, afectando a colectivos minoritarios o a pequeñas empresas o negocios que se ven abrumados ante el fenómeno del "*Big Data*". La discriminación resulta de la aplicación de los parámetros empleados para filtrar y jerarquizar los datos, es decir, a través de la utilización de algoritmos para la toma de decisiones[6] se generan situaciones que no son imparciales o neutras. Con la creación de esos algoritmos se establecen determinados juicios de valor, creencias, ideas políticas, intereses económicos… esto es así porque el uso de los algoritmos esta optimizado para lograr un determinado objetivo en favor del ente que lo emplea.

El Parlamento Europeo en relación con la discriminación presentó a través de una resolución[7] una petición tanto a la Comisión como a los Estados miembros para que adoptaran todas las medidas necesarias para evitar o minimizar la discriminación creada por los algoritmos además de marcar un ambiente ético común en el que se dé un tratamiento transparente de los datos personales. Esta idea que plantea el Parlamento Europeo es muy

[6]De la Agencia Europea para los Derechos Fundamentales*: "Big Data: Discrimination in data-supported decisión making",* Austria, 30 de mayo de 2018 disponible en https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-focus-big-data_en.pdf

[7]Resolución del Parlamento Europeo, de 12 de febrero de 2019, sobre una política industrial global europea en materia de inteligencia artificial y robótica (2018/2088)

relevante ya que se puede plantear la discriminación de ciertos grupos. Por ejemplo, en el caso de determinados grupos religiosos que descartan el uso de anticonceptivos y son más propensos a engendrar hijos, esto puede ser detectado indirectamente por el algoritmo y descartar la contratación de los miembros de ese grupo por tener más posibilidades de tener hijos y consecuentemente tener derecho a permisos por paternidad o maternidad que podrían afectar a la empresa que contrata.

Por último, es oportuno destacar las conclusiones sacadas del Grupo de trabajo[8] de protección de las personas en lo que respecta al tratamiento de datos personales, centrado en el Reglamento General sobre protección de datos, concretamente en el artículo 37.1 del Reglamento General, las cuales vienen a establecer la necesidad de la figura de los delegados de protección de datos[9], cuyo objetivo será que se cumpla el Reglamento General. Se deberá realizar un control de las actividades de los organismos públicos, así como de las actuaciones principales de los responsables o encargados del procesamiento de datos. El delegado tendrá acceso tanto a los datos personales como a los procesos de tratamiento. Además, su función se centrará en realizar una labor de información y asesoramiento con los sujetos que procesen los datos y cooperará con la Agencia Española de Protección de Datos.

Se establecen además una serie de protocolos y procedimientos de actuación que tendrán que seguirse cuando se recopilen datos personales y característicos de una persona, con el fin de garantizar así la correcta captación y uso de la información. Será el delegado de protección el que tendrá que obtener el consentimiento del sujeto afectado para proteger de esta forma sus derechos fundamentales. Además, en relación con el consentimiento, los datos obtenidos habrán de procesarse siempre en el marco para el que se obtuvieron, es decir, no se puede emplear la información obtenida a través de un consentimiento que se otorgó para una determinada finalidad para otros objetivos. Por ello, el Reglamento General trata de brindar una protección cuantitativa, desde el punto de vista de limitar la acumulación de los datos a los necesarios para la actividad consentida.

Por último, se menciona un aspecto de gran importancia y es el acceso a la información recabada, una tarea basada en la transparencia, el sujeto que ha aportado sus

[8]Grupo de Trabajo sobre Protección de Datos del artículo 29 creado por la directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995

[9]Funciones del Delegado de Protección de Datos, disponible en: http://www.poderjudicial.es/cgpj/es/Servicios/Atencion-Ciudadana/Delegado-de-Proteccion-de-Datos/

datos ha de tener acceso a ellos para controlar si ha existido un exceso en la obtención de los mismos, y, por tanto, se ha podido ver vulnerado alguno de los derechos que le asisten.

En conclusión, las tareas del Grupo de Trabajo van encaminadas a la unificación de la regulación e interpretación común de todos los Estados miembros en materias relativas a la protección de datos. Si bien es cierto que las medidas aquí comentadas no son vinculantes, sí son recomendables, pudiendo ser empleados los criterios del Grupo de Trabajo por los legisladores y Tribunales. El objetivo es garantizar la aplicación de Reglamento General de Protección de Datos, controlando la acción de los captadores y procesadores de información con sede en la UE. También puede aplicarse la regulación a organizaciones, que, sin sede en la Unión, traten datos de residentes en la UE. Todas las medidas van encaminadas a garantizar la seguridad de la información bajo los principios de integridad y confidencialidad, recogidos en el artículo 5 del reglamento. En base a esto considero que el afán de estas medidas es adecuado pero que a la vez se plantea como un reto, por lo novedoso del asunto, y además por el hecho de que se recurre a la colaboración de las organizaciones que tratan los datos, no siendo posible garantizar una transparencia absoluta. En este sentido, las sanciones por no adoptar medidas de seguridad pertinentes o por no nombrar un delegado de protección de datos van desde los 10 millones hasta el 2% del volumen del negocio total anual de la empresa o, por otra parte, de 20 millones hasta el 4% del volumen del negocio total anual por vulnerar los derechos relativos a protección de datos. Estas sanciones tienen un impacto importante que trata de garantizar el establecimiento de medidas y la protección de datos.

2.2 ¿Cómo afecta a la democracia?

En este punto vamos a tratar la influencia del *Big Data* dentro de la democracia[10] entendiendo esta como un sistema político[11] en el que la soberanía estatal reside en el pueblo que será quien decida y controle a sus gobernantes. Cabe diferenciar entre democracia representativa y democracia directa y es el avance de la tecnología el que ha conseguido que se abra el debate sobre qué tipo es posible y más adecuado a los tiempos que corren.

[10]GARCIA F.: "*Big Data y democracia*" en Revista internacional de Filosofía núm. 23, 2019, pp. 114 a 134

[11]SARTONI, G.: *"¿Qué es la Democracia?",* ed. Penguin Random House, Ciudad de México, 2012, pp. 8 y ss.

Como primera idea podemos plantear el uso dentro de la democracia de las tecnologías[12] para la toma de decisiones a través de consultas populares que puedan ser tenidas en cuenta por los representantes políticos a la hora de legislar sobre determinadas materias. Esta idea encuentra su apoyo en España en el artículo 23 de la Constitución Española, donde se brinda a los ciudadanos el derecho a participar en los asuntos públicos, debiendo entender este articulo como que se brinda la posibilidad de elegir a sus representantes o presentarse como tal, es decir, sufragio pasivo y activo. Y es en esta idea en la que se asienta nuestra democracia Constitucional en la participación en los asuntos públicos por medio de representantes. Por otra parte, los mecanismos de democracia directa quedan reducidos a supuestos como la reforma constitucional en que se plantea como necesario un referéndum dentro del procedimiento.

Uno de los pilares fundamentales de nuestro Estado es la consideración de democrático, residiendo la soberanía en el pueblo, que la cede en favor de unos representantes. La realidad es que nuestra sociedad se organiza en torno a los representantes políticos, debido a la imposibilidad de tomar decisiones en conjunto. La tecnología rompe con esta idea facilitando la conexión y, con esa conexión, aparecen medios de participación política directa. En el idílico supuesto, en el que se posibilita una democracia directa, podría plantearse la influencia que podrían tener las distintas organizaciones a través del uso del *Big Data*. El riesgo puede venir del uso del *Big Data* para la creación de determinadas tendencias, esto sucede al emplear la información procesada para inducir ideas en determinados sujetos. Las decisiones de las personas pese a parecer tomadas libremente están influidas por los sujetos que controlan el uso del *Big Data*. Como conclusión sobre este debate entre democracia directa y representativa, en el marco de este trabajo, quiero dejar la idea de que existe un alto riesgo de creer que se toman decisiones libremente cuando en realidad esas decisiones vienen marcadas por la información que nosotros estamos vertiendo a la red, y, por lo tanto, no es una decisión tomada libremente si no influida en gran medida por el órgano estatal o privado que sea capaz de controla el *Big Data*. Se tratan por tanto de decisiones basadas en *Big Data* que "*tratan de inducir a las personas determinados valores y patrones de conducta deseables en una determinada sociedad*" [13], ya que a través del procesamiento de la información descubren que comportamientos y opiniones son más deseables. Por ello, parece imposible que la democracia representativa ceda a favor de la democracia directa,

[12]CUADRA-SALCEDO, T.: "*Retos, Riesgos y Oportunidades de la Sociedad Digital*" en QUADRA-SALCEDO, T/PIÑAR, J L. (Dirs): "*Sociedad Digital y Derecho*" ed. Red.es y BOE, Madrid, 2018, pp. 21 y ss.

[13]O´NEIL, C.: "*Armas de destrucción matemática*" ed. Crown Books, EE.UU.,2016 pp. 198

simplemente podrá complementarla para tomar ciertas decisiones y encontrar opiniones de los ciudadanos que se traducen en una fuente de información útil para optimizar la propaganda electoral.

Centrándonos en nuestra democracia representativa, y, en esta última idea, el *Big Data* puede tener un papel importante dentro de nuestro sistema político para su uso en campaña electoral que, pueden verse marcados por la elaboración de perfiles y la adopción por partidos políticos de políticas destinadas a conseguir el voto de ciertos votantes con un determinado perfil. Y es que en la era de la tecnología es lógico que con el fin de alcanzar al mayor número de votantes se formule una campaña electoral enfocada en agradar al mayor número de personas dispuestas a votar. Se trata de conocer las ideas más populares y con mayor aceptación ciudadana para conseguir la confianza de los votantes. Se busca el perfil del votante mayoritario y se estudian las distintas posibilidades para incidir en esos aspectos en campaña. Pionero en este tema fue Barack Obama[14] quien en 2012 empleó el *Big Data* a través de su administración "*we the people*" realizando numerosas encuestas con las que logró una cercanía con los ciudadanos que se tradujo en un flujo altísimo de información para su posterior uso en campaña. Su intención era emplear esta información para ser más competitivo respecto a sus rivales políticos, la idea era básicamente recopilar información que se encontraba en la web en relación con las distintas medidas que se proponían y tratar de asegurar a los votantes más indecisos, ajustando su programa electoral a través de la inclusión de medidas que más preocupaban a la población.

Este uso se ha ido extendiendo y en la actualidad se plantea como pilar fundamental de las campañas políticas de los distintos partidos políticos en los diferentes países. Esta generalización supone un riesgo claro dado que viene a abrir la puerta a que determinados grupos obtengan poder a través de la búsqueda del perfil del votante mayoritario para orientar en ese sentido sus políticas y ganar su confianza, pudiendo aplicar políticas diferentes una vez gozan del poder logrado.

En este punto cabe plantearse la idea de que el uso del *Big Data* en estos ámbitos puede ajustarse a una conducta prohibida por la ley General de Publicidad 34/1988, que en su artículo tres prohíbe la publicidad ilícita. Esta misma ley define la publicidad subliminal como la publicidad que "*mediante técnicas de producción de estímulos de intensidades fronterizas con los umbrales de los sentidos o análogas, pueda actuar sobre el público destinatario sin ser conscientemente*

[14]JIN X,WAH BH, CHENG X,WANG Y.: "*Significance and Challenges of Big Data Research*" en "*Big Data Research*" núm. 2, 2015, pp. 61 y ss.

percibida". Aquí el *Big Data* resulta muy útil, ya que permite emplear la información para dejar atrás técnicas prohibidas, y abrir la puerta a una publicidad personalizada acorde a las necesidades de la gente. Pero esta personalización y perfección de las técnicas publicitarias pueden llevar también a otro escenario que es el del uso de publicidad subliminal personalizada, siendo muy convincente y resultando tremendamente efectivo. Es por esto que no parece descabellado que el uso del *Big Data* pueda incurrir en la vulneración de normas que prohíben estas técnicas.

Por otra parte, es una realidad que los gobiernos estatales tratan de realizar una gestión transparente y, muchos, emplean el "*open government*"[15] como método para superar la opacidad y fortalecer la democracia. Se trata de una técnica basada en la transparencia y participación de los ciudadanos gracias a los medios tecnológicos. Una de las formas de facilitar el acceso a los datos de las administraciones públicas es el desarrollo de portales informáticos donde alojan las bases de datos. Las administraciones públicas emplean la información para argumentar sus acciones y establecer planes estratégicos.

La relación con el Big Data reside en que las administraciones emplearán técnicas de procesamiento de datos para gestionar toda la información y tomar decisiones en su ámbito. Esta técnica se ha denominado "inteligencia territorial" y puede resultar determinante entre el desarrollo de un territorio y otro, ya que el desarrollo de las comunidades se realiza de forma más optima si se emplean los datos procesados para la toma de decisiones. Además, una gestión más optimizada contribuye a la transparencia de la gestión y, a su vez, supone una democracia más participativa. El hecho de que el gobierno permita a los ciudadanos el acceso a sus datos supone que la sociedad se sentirá participe de la gestión. Todo esto contribuye a una gestión optimizada de los servicios públicos y, en definitiva, una mejora de estos.

Por último, hay que incidir en el riesgo de la creación de un submundo digital en relación con el Estado, el cual está lleno de ventajas, pero también desventajas, y es que las formas de participación en la vida política y acceso a servicios estatales a través de las tecnologías resulta de gran utilidad, pero también suponen un riesgo y es que se almacenan grandes cantidades de información en ese "mundo digital" lo que supone un riesgo para el Estado y los ciudadanos. Hay que tener en cuenta que existe tal cantidad almacenada que en malas manos puede resultar un riesgo para la economía, el mercado, la sanidad, etc. En este

[15]DURÁN, F.J.: "Big Data aplicado a la mejora de los servicios públicos y protección de datos personales" en Revista de la Escuela Jacobea de Posgrado, núm. 12, 2017, pp. 46 y ss.

punto, tenemos que conocer que nuestro sistema sanitario se encuentra conectado para poder actuar más rápido en las diferentes situaciones, esto es así puesto que nuestro historial clínico que se encuentra disponible en la nube gracias a la tecnología, pero esa información ha de estar protegida por lo personal e importante que resulta esa información. Es por ello que el Estado habrá de destinar gran parte de sus esfuerzos a la protección de esta información y legislar sobre materias que puedan resultar atípicas pero que con los avances tecnológicos se encuentran a la orden del día.

Para terminar con este apartado quiero comentar la influencia que puede llegar a tener el *Big Data* en la idea de "*checks and balances*"[16] que podemos relacionar con la idea de separación de poderes, y es que el *Big Data* puede emplearse como cortafuegos para evitar las posibles influencias sobre los distintos poderes. Toda la información puede ser empleada para que los gobiernos de los diferentes Estado actúen de forma más eficiente y para que se garantice la transparencia de su gestión. De esta forma, se puede emplear el *Big Data* dentro de la democracia para que las opiniones vertidas por los ciudadanos se valoren y sean tomadas en cuenta por el Estado para actuar de forma más eficiente sirviendo a los intereses de los ciudadanos de ese Estado que al final deben ser los intereses a los que los representantes políticos en una democracia han de servir.

El *Big Data* podrá ser empleado en relación a los "*checks and balances*" para analizar diferentes datos y establecer algoritmos que identifiquen conductas tendentes a la concentración de poder. Así mismo, se podrá emplear el *Big Data* con una finalidad preventiva si se utilizan algoritmos para la toma de decisiones y evitar que interfieran voluntades no deseadas.

A parte del uso en aras de mejorar la eficiencia de los Estados, cabe incidir en la idea de que el *Big Data* podrá emplearse como control de las actuaciones que llevan a cabo los Estados, esto vendría a ser el uso de la información sobre distintos asuntos que llevan a cabo las administraciones y garantizan la transparencia. Un ejemplo[17] del uso que se puede dar a la tecnología del *Big Data* en nuestro país sería el posible control de los actos discrecionales de las entidades públicas que rompen con el derecho administrativo a la hora de realizar concesiones administrativas para realizar obras públicas o prestar determinados servicios según la conveniencia y con total discrecionalidad. Ante estos actos discrecionales puede

[16]BARNETT H.: "*Constitutional and Administrative Law*", ed. Taylor & Francis, Londres, 2019, pp. 76 a 86

[17]MARÍN H.: "*Discrecionalidad administrativa*", ed. Universidad Externado de Colombia, Bogotá, 2007, Capítulo II: "*Concepto de discrecionalidad administrativa*"

emplearse el Big Data[18] para identificar estas conductas o incluso para prevenirlas, empleando algoritmos para la asignación de concesiones. De esta forma se reduce la discrecionalidad eliminando ciertos aspectos subjetivos, optimizando el proceso y logrando que las decisiones tomadas se ajusten a los criterios que se buscan y no a la voluntad, en algunos casos viciada, de quienes llevan a cabo la concesión.

2.3 ¿Cómo afecta al mercado?

En cuanto al análisis de la incidencia del *Big Data* en el mercado, es preciso partir de la evidente influencia que presenta la tecnología en el mercado al facilitar la conectividad entre las personas. Esta conectividad tiene como consecuencia la eliminación de ciertas barreras físicas y, por lo tanto, se facilita de manera enorme el comercio. Las facilidades mencionadas dan pie a nuevos problemas como pueden ser los fiscales, ya que se complica la determinación de la actividad desarrollada y el lugar en que se realiza. Esta influencia se ve reflejada en la forma en que los elementos del mercado se han visto afectados por los avances tecnológicos. Partiendo de los productos y servicios que se ofertan, estos gozan de mayor visibilidad gracias a la tecnología siempre y cuando se empleen técnicas de *marketing* correctas y adaptadas a nuestros tiempos, así como una pérdida de importancia del contacto físico para conocer el producto o servicio en cuestión. Es por ello que los vendedores habrán de implementar el uso de tecnologías para así lograr una mayor competitividad en el mercado, identificando los gustos de los consumidores y tratando de satisfacer los mismos, así como potenciar la publicidad que se dé sobre sus productos y servicios.

La tecnología también habilita herramientas que permiten llevar a cabo un control preciso de factores del mercado como el precio, la oferta y la demanda. Esta nueva forma de análisis hace que el uso *Big Data* pueda marcar la diferencia, siendo más competitivos los sujetos que empleen estas tecnologías. Surgen tecnologías de "*sensemaking*"[19] que básicamente llevan a cabo una función recopiladora de datos para realizar un análisis de la situación, con datos tanto de la empresa como de aspectos externos, y poder tomar decisiones rápidas y acertadas.

[18]SOLIS, V: "*Técnicas de inteligencia artificial para optimizar la eficiencia del procedimiento de selección para la contratación de obras públicas*" en Revista Interfases, núm. 11, 2018, pp. 13 y ss.
[19]GIL, E.: "Big data, privacidad y protección de datos" ed.: AEPD y AEBOE, Madrid, 2016, pp. 136

Es aquí donde aparece una nueva cuestión, y es que la aplicación de las normas que regulan el mercado habrán de adaptarse a estas tecnologías y tendrán que cubrir los aspectos que se plantean a causa de la tecnología y no estén regulados. Y es aquí donde en la actualidad[20] vemos la aparición de empresas punteras en el ámbito tecnológico que se consolidan como las mayores empresas del mundo, por el control y enfoque que han sabido dar con estas nuevas tecnologías y el uso del *Big Data*. Con todo esto nos plantamos en una situación actual en la que se ha producido un cambio de modelo de negocio en el que se premia el uso de la tecnología y en el que se abre la puerta a un nuevo marco comercial y legal bajo la transposición del mercado a Internet. El uso de técnicas de *Big Data* en este entorno parece que además de ser útiles para optimizar las políticas de venta y publicidad, pueden otorgan una clara ventaja competitiva.

Uno de los principales problemas que atañen al mercado es la concentración de la información, del *Big Data*, en las grandes empresas, las cuales a través del procesamiento de esos datos pueden afectar al mercado y a la competencia. El uso de *Big Data*[21] puede actuar en un primer lugar como una barrera de entrada, limitando el acceso al mercado, esto se plasma en la idea de que para el acceso al mercado se necesita actualmente que una gran parte del negocio que pretende entrar en el mercado destine sus recursos al procesamiento y gestión de datos, esto hace que se tenga que recurrir a empresas de gestión de *Big Data* lo que, en algunos casos, supone algo imposible para determinados negocios. El hecho de que ciertos negocios no puedan afrontar esta gestión del *Big Data* supone la aparición de una barrera de entrada ya que tratar de acceder al mercado sin apoyarse en el *Big Data* supone una desventaja competitiva infranqueable. Por otra parte, es una realidad que el acceso a la información no es exclusivo, es decir, la posesión por una empresa de la información recopilada no supone la imposibilidad de acceso a la misma por otra empresa[22], aunque bajo mi punto de vista siempre existirá una ventaja clara e insuperable que venga a crear una barrera de entrada a ciertas empresas o negocios que quieran entrar en el mercado. Un claro ejemplo de ello viene a darse en los mercados de doble cara, en el ámbito del comercio, empresas como Amazon realizan una labor de gestión por un lado de los consumidores,

[20]CUADRA-SALCEDO, T.: "*Retos, Riesgos y Oportunidades de la Sociedad Digital*" en QUADRA-SALCEDO, T/PIÑAR, J L. (Dirs): "*Sociedad Digital y Derecho*" ed. Red.es y BOE, Madrid, 2018, pp. 21 y ss.

[21]HERRERO SUAREZ C.: "*Big Data y Derecho de la competencia*" en QUADRA-SALCEDO, T/PIÑAR, J L. (Dirs): "*Sociedad Digital y Derecho*" ed. Red.es y BOE, Madrid, 2018, pp. 659 y ss.

[22]Competition Law and Data, 2016, Gemeinsames Papier der Autorité de la concurrence und des Bundeskartellamtes zu Daten und Auswirkungen auf das Wettbewerbsrecht: https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Berichte/Big%20Data%20Papier.html

ofreciendo atención y productos personalizados y por otra parte dando escaparate a determinados comerciantes. La labor que lleva a cabo Amazon a través del procesamiento de datos se plantea imposible para una empresa que decida aparecer en el mercado, quedando su posición reducida a depender de que Amazon decida brindar ese escaparate a nuevas empresas para comercializar sus productos. Es decir, se necesita una gran cantidad de recursos y ello no asegura el éxito ya que el riesgo de entrar en un mercado tan marcado por la conexión y la tecnología es tan alto que supone en muchos casos una barrera de entrada.

Otro aspecto a tener en cuenta a raíz del ejemplo comentado es la condición de las empresas que aprovechan el procesamiento de datos y gracias al uso del *Big Data* pasan a tener una posición dominante en el mercado[23], entendida como situación de poder económico, en este caso, basada en la acumulación de información, por parte de una empresa que hace que tenga una capacidad de control tal que puede afectar a la competencia en el mercado. El artículo 2 de la ley 15/2007 de defensa de la competencia prohíbe el abuso de posición dominante[24] en general ya sea en la imposición de precios y condiciones en el mercado u afectando de otras formas al mercado. Parece evidente la relación que existe entre la cantidad de información disponible y poder en el mercado, pero esto no es del todo cierto, ya que la información habrá de ser procesada de forma adecuada y habrá de tener un contenido cualitativo para poder emplear esa información de manera eficiente. La calidad de la información recopilada tiene un papel importante a la hora de considerar la posición dominante, ya que se dará cuando la información captada pueda ser empleada de tal forma que resulte útil y por tanto brinde ese poder a quien la posea. En este punto, parece claro que a través del procesamiento de ciertos datos relevantes puede realizarse un estudio rápido y eficaz de aspectos del mercado como la oferta y la demanda, y con estos datos llevar a cabo acciones como la fijación de precios que puedan obstaculizar la libre competencia. La colusión se puede dar debido a que al existir una mayor cantidad de información sobre el funcionamiento del mercado pueden emplearse algoritmos que vengan a establecer los precios. Esto se plantea desde la perspectiva de que empresas, de manera consensuada junto a otras empresas o simplemente fruto del uso del mismo tipo de algoritmo, pueden llevar a cabo prácticas de fijación de precios bajo la técnica del "*dynamic pricing*" en función de la actividad del mercado y de las acciones que lleven a cabo otras empresas. El análisis de estas

[23]CLAICI, A.: "*Big Data y Política de la Competencia*" en Papeles de Economía Española, nº 157, 2018, pp. 261

[24]KÖRBER, T.: "*Data, Platforms and Competition Law*", disponible en: https://ec.europa.eu/competition/information/digitisation_2018/contributions/torsten_koerber.pdf

conductas se complica y demostrar que esas conductas han sido pactadas puede resultar imposible ya que responden a algoritmos extendidos por las empresas para lograr optimizar su rendimiento. La idea del "*dynamic pricing*" es emplear la información que se recopila sobre el mercado y emplear esa información para ajustar los precios a esas circunstancias. La cuestión es que esta técnica puede tener un trasfondo que suponga la fijación de precios, conducta prohibida en el artículo 101.1 a) del Tratado de Funcionamiento de la UE. Al no existir un control legal sobre esta técnica no se puede garantizar que el ajuste de los precios no se esté haciendo de forma consensuada no solo valorando los datos que te brinda el mercado, sino que además puede responder a verdaderos consensos entre empresas para variar los precios y así brindar una falsa realidad de competencia, cuando en realidad se ha establecido un acuerdo[25] por el que a través del uso de esos logaritmos se realiza una fijación de precios, rompiendo con la oferta y la demanda y actuando la voluntad del algoritmo, y con ello la de las empresas. Esta idea en un principio difícil de contemplar se plantea como posible en este entorno globalizado por las nuevas tecnologías y es que resulta indiferente como se exprese la voluntad, lo que importa es el contenido, es decir, la voluntad de fijar unas pautas, un comportamiento en el mercado.

Parece entonces que el *Big Data* puede resultar un peligro para la economía de mercado y la competencia efectiva. También se plantea otra incidencia que viene a ser la posibilidad de emplear el *Big Data* para el reparto de mercados, conducta prohibida por la ley 15/2007 que en su artículo 1. El hecho de conocer como el mercado responde en según qué ámbito a determinadas empresas puede resultar muy útil para que una empresa enfoque su trabajo hacia un determinado mercado y con ciertos productos o servicios, pero esta información y estos pronósticos pueden llevar a conductas por parte de las empresas mediante las cuales se haga un reparto de mercado en función de los resultados más favorables que se prevean. Además, existe la posibilidad de que el uso de estos algoritmos[26] lleve a conductas no pactadas expresamente por las empresas pero que incurran en conductas anticompetitivas.

Otro aspecto en el que se ha visto reflejada la importancia del *Big Data* ha sido es en el interés que muestran las empresas por adquirir información. Esto se puede ver en el caso de Facebook que adquirió la plataforma Whatsapp, un servicio gratuito, pero que contiene

[25]CLAICI, A.: "Big Data y Política de la Competencia" en Papeles de Economía Española, nº 157, 2018, pp. 260

[26]MARTINEZ, MC.: "*Algoritmos, Big Data y el derecho de la competencia*" disponible en: https://www.asuntoslegales.com.co/analisis/maria-claudia-martinez-beltran-402342/algoritmos-big-data-y-el-derecho-de-la-competencia-2551051

un alto contenido en información y esta información puede ser de una calidad y valor muy alto, por ello las autoridades de la competencia analizaron esta operación y finalmente aceptaron la adquisición.

Conociendo todos estos supuestos parece evidente que la legislación sobre derecho de la competencia, así como la CNMC (Comisión Nacional de los Mercados y la Competencia) habrán de atender a las posibles situaciones en las que pueden desembocar el uso de la tecnología del *Big Data* para adaptarse a nuevas situaciones anticompetitivas y poder cubrir estas nuevas conductas colusorias.

Hasta este punto hemos valorado el uso del *Big Data* en conductas que pueden resultar restrictivas de la competencia, pero, por otra parte, cabe emplearse esta tecnología para analizar las conductas que se lleven a cabo en el mercado y con ello garantizar el cumplimiento de la normativa relativa a la competencia. Se plantea la posibilidad de emplear esta información para evitar la comisión de conductas prohibidas, así como detectar posibles conductas colusorias. Se brinda por tanto una buena herramienta en manos de las autoridades de la competencia para poder analizar y detectar conductas que atenten contra el mercado y la competitividad. El uso de *Big Data* supone poder captar y procesar datos relativos a elementos como pueden ser el precio, la oferta o la demanda, así como las conductas que llevan a cabo las empresas y, con ello, poder elaborar algoritmos para identificar conductas prohibidas y favorecer la aplicación del derecho de la competencia.

La realidad actual es que no se está prestando la suficiente atención al *Big Data* como herramienta que puede llevar a determinadas conductas que pueda dañar el mercado, son pocos los casos en que empresas se están viendo cuestionadas por el uso del *Big Data* en el mercado, aunque sí que hay algunos casos como el de "*Bundeskartellamt*", órgano alemán en defensa de la competencia, que impuso a Facebook ciertas restricciones en la recopilación y procesamiento de datos, ya que el uso que se estaba dando a esa información era desconocido por los usuarios y estaba generando un abuso de la posición de poder que ostenta la empresa. No se trata de una decisión tomada por un tribunal y resulta criticable que este órgano entre a valorar aspectos como el tratamiento de datos que Facebook hace, así como el procesamiento conjunto de los datos obtenidos en varias de sus plataformas. Y aunque parece evidente que la posesión de tal cantidad de información supone una posición de poder en el mercado, esto puede no ser del todo cierto, y aun siendo cierto, habría que demostrar que el uso de ese poder de una forma abusiva, lo que, en virtud de los supuestos en este apartado mencionados, se plantea como una posibilidad.

Por todo esto, y como conclusión, parece necesario que se abra la puerta a una nueva forma de analizar que rompa con los métodos de análisis tradicionales y tenga en cuenta estos escenarios marcados por la tecnología para analizar las posibles conductas colusorias.

2.4 ¿Cómo afecta a los medios de comunicación?

Parece claro que la tecnología ha venido a crear un nuevo panorama que ha roto totalmente con lo tradicional. Esta ruptura plantea gran importancia debido a que los medios de comunicación[27], el "cuarto poder", ha perdido importancia con el avance de las nuevas tecnologías. La facilidad de acceso a medios electrónicos o redes sociales permite conocer datos a tiempo real comentados por multitud de personas que han encontrado en las redes sociales un instrumento muy útil y accesible, gracias a la gratuidad de sus servicios y su facilidad de uso. Esto supone una limitación a los medios tradicionales, ya que, pese a que parece perfectamente compatible la sostenibilidad de los medios tradicionales y la de las redes sociales, esto no es del todo cierto. Las redes sociales, junto con los medios digitales, han venido a concentrar la publicidad[28], gracias a que su uso se ha extendido, y esta ganancia ha llevado a la perdida de publicidad y financiación de los medios tradicionales.

La pérdida de estos medios tradicionales puede suponer la vulneración de derechos como la libertad de expresión y libertad de prensa, así como el derecho a la información. El Tribunal Constitucional señala[29] que el derecho a la información "*no solo protege un interés individual*" sino que además habrá de salvaguardar este derecho para que se garantice la existencia de una opinión publica libre que está asociada, indisolublemente, a nuestra democracia.

La creación de plataformas como YouTube, Netflix… han venido a romper con la hegemonía de la televisión ya que, aparte de innovar y brindar multitud de servicios, han generado una forma de obtención de información que posteriormente puede ser vendida o procesada en su propio beneficio. Esto ha sido apreciado por los medios tradicionales que han adaptado sus servicios al mundo digital, en muchos casos de forma gratuita, obteniendo

[27]FERNÁNDEZ E.: "*Big Data: Eje estratégico en la industria audiovisual*" ed. UOC, Barcelona, 2017 pp. 98 y ss.
[28]RUBIO, R.: "*El Derecho a la información y el derecho al voto*" en QUADRA-SALCEDO, T./PIÑAR, JL. (Dirs): "*Sociedad Digital y Derecho*" ed. Red.es y BOE, Madrid, 2018, pp. 467 y ss.
[29]STC 68/2008, de 23 de junio, fundamento jurídico 3º

una nueva fuente de recursos, en este caso, información. Es en este punto en el que entra en juego el *Big Data*, ya que los medios de comunicación han tenido que hacer una doble adaptación, por una parte, de su contenido, y por otra, han tenido que promover técnicas de procesamiento de datos para con ello obtener un rendimiento.

El uso de las redes sociales o estos medios digitales, en sustitución de los medios tradicionales, tiene un doble riesgo, por un lado, el mencionado en relación con la cesión de información para su uso que se traduce en la recopilación de información de gran valor por parte de las empresas. Por otra parte, el evidente riesgo que se plantea respecto a su contenido que esta básicamente formado por las vivencias u opiniones de sus usuarios. La información que encontramos en las redes no tiene filtro, lo cual hace que su veracidad se ponga en duda. Junto a esto, se unen las posibles difusiones de información engañosa o ficticia generando campañas de desinformación sistemática, lo que de forma organizada puede llegar a influir en situaciones como las elecciones.

Para finalizar este apartado, hay que considerar la idea de que los medios de comunicación tradicionales también pueden sacar provecho del *Big Data* a la hora de optimizar sus emisiones y el contenido que van a ofrecer. Se trataría por tanto de recuperar la función del "*cuarto poder*"[30] como "*instrumento para encauzar la opinión pública*" a través de la optimización de su contenido, sin olvidar que la posible influencia por poderes políticos o estatales va a estar controlada por los ciudadanos que tendrán capacidad de mostrar estar influencias a través de redes sociales, actuando como "*checks and balances*". Los medios tendrán que utilizar las redes sociales como contacto con los telespectadores, para que interactúen con los programas y muestren sus preferencias, toda esta información puede analizarse para detectar picos de audiencia y de actividad para dar un servicio optimizado y obtener el mejor rendimiento posible a sus emisiones. A través de este procesamiento de información, empleando técnicas de *Big Data* puede llegar a garantizarse un efectivo derecho a la información y con ello garantizar la pluralidad política y de opiniones, aspecto muy relevante en un Estado Democrático.

[30]CUADRA-SALCEDO, T.: "Retos, Riesgos y Oportunidades de la Sociedad Digital" en QUADRA-SALCEDO, T./PIÑAR, JL. (Dirs): "Sociedad Digital y Derecho" ed. Red.es y BOE, Madrid, 2018, pp. 33 a 35.

2.5 Necesidad de tribunales especializados

La legislación europea establece que los tribunales especializados[31] serán aquellos órganos que se encarguen de tratar en primera instancia determinados asuntos que según qué materias necesitan ser tratadas por un órgano especializado. Estos tribunales dependen del Tribunal de Justicia de la Unión Europea, adjuntos al Tribunal General. Respecto a la creación de los mismos responde a razones de necesidad de abordar determinadas materias desde una perspectiva más concreta y son creados mediante reglamento que tendrá que ser considerado y aprobado por la Comisión y, conjuntamente en la decisión participará además el Parlamento. Para la aprobación de estos tribunales, el reglamento por el que traen causa requiere la aprobación mediante una mayoría cualificada. Así mismo, respecto a su composición, los miembros de este órgano serán personas que cumplan los requisitos de independencia, así como la capacidad y especialización necesaria para llevar a cabo esas funciones, siendo el consejo quien por unanimidad decida la composición de los mismos. Mencionar que, pese a la existencia de esta posibilidad, solo se ha creado un tribunal especializado que actualmente se encuentra disuelto y fue el Tribunal de la Función Pública.

En este punto quiero mencionar la tarea que lleva a cabo el Tribunal General respecto a los asuntos referidos al complimiento del Derecho de competencia, y es que este Tribunal ha venido a imponer sanciones en relación con abuso de posición dominante, como es el caso Microsoft tras haber impuesto la Comisión una sanción por restringir la divulgación de cierta información de interés para la creación de software alternativo al proporcionado por Microsoft. Así como otros asuntos, como el caso en que Microsoft adquirió la plataforma Skype y sus competidores consideraron esa fusión como limitadora de la competencia, lo que fue llevado al Tribunal General que declaró que esa conducta no limitaba la competencia.

A razón de todo lo anterior, considero que, ante la novedad del asunto del *Big Data*, podría ser razonable llevar a cabo la creación de un Tribunal Especializado que venga a tratar los asuntos en que puedan verse comprometidas las normas europeas, no solo a nivel de derecho de la competencia sino también a nivel incluso de la protección de datos[32]. Si bien es cierto que el TJUE en principio no brinda una protección específica a los derechos humanos, y, con ello a la protección de datos, sí defiende los intereses del Derecho de la Unión Europea, así como extender una interpretación uniforme de la legislación, es decir,

[31]Definición de Tribunales Especializados, según el glosario del Derecho de la Unión Europea: https://eur-lex.europa.eu/summary/glossary/specialised_court.html?locale=es

[32]Protección de datos y privacidad online, disponible en: https://europa.eu/youreurope/citizens/consumers/internet-telecoms/data-protection-online-privacy/index_es.htm

del Derecho de la Unión en el que se incluye la *Carta de los Derechos Fundamentales de la Unión Europea*[33]. En el artículo 8 de esta Carta se reconoce la protección de datos de carácter personal, así como la regulación sobre la circulación de estos datos, regulando aspectos como el modo de tratamiento que ha de ser leal y para unos fines concretos y siempre habrán de estar obtenidos teniendo en cuenta la voluntad de la persona a quien se refieren, es decir, mediando consentimiento.

Por todo lo comentado anteriormente y en base al desconocimiento y la ausencia de regulación específica, considero que debería valorarse la necesidad de crear tribunales especializados en el ámbito del *Big Data* para dar solución a aspectos novedosos y de complejo análisis que se puedan dar de aquí en adelante y con ello anticiparse a las posibles situaciones que comprometan tanto el Derecho de la competencia como los derechos fundamentales.

2.6 Vulnerabilidad de la información: "ransomware"

Para terminar este capítulo conviene subrayar la idea de que la información sobre la que se basa el *Big Data* tiene un gran valor y por ello tantos los órganos privados como públicos optimizan la obtención y procesamiento del mismo, pero una vez conseguida esta información también ha de ser protegida de una forma especial, para garantizar así la seguridad de las personas y evitar usos no deseados.

Parece que el primer riesgo recae en la fuente de esta información, las personas se encuentran en ocasiones desprotegidas en el mundo de Internet, en muchos casos por la aceptación de determinadas cláusulas que no son claras o comprensibles y en otros casos puesto que la información es sustraída sin el consentimiento de los usuarios. El simple acto de hacer un "clic" puede suponer la puesta en riesgo de información comprometida y muy valiosa, y ese aspecto habrá de ser regulado y tenido en cuenta, puesto que la seguridad que brinda nuestro sistema jurídico tiene que llevarse y alcanzar al marco de Internet.

Por otra parte, el segundo riesgo se centraría en los órganos que obtienen y procesan nuestra información, ya que una vez obtenida esta información debe ser almacenada y protegida. De lo contrario, los ciberdelincuentes, podrían tener acceso directo a la

[33]Carta de los Derechos Fundamentales de la Unión Europea de 26 de octubre 2012

información de multitud de personas mediante la apropiación de una única unidad de datos almacenados. Si bien es cierto que encontramos cierta regulación en el *Reglamento General de Protección de Datos de la Unión Europea*[34], relativa a normas de privacidad, que obligan a las empresas en relación con el *Big Data* a tener una diligencia y protección sobre la información que tienen almacenada. En este punto está claro que tanto el acceso como el almacenamiento de la información habrá de estar controlado para garantizar la seguridad y eliminar posibles filtraciones de información.

Es en este último punto es donde aparece el concepto "*ransomware*"[35] entendido como "*malware*", es decir una amenaza informática[36], que lo que viene a hacer es limitar el acceso o sustraer la información privada de las personas para posteriormente pedir un rescate de la información. Se establece como un nuevo tipo de "secuestro" de información a través de Internet que puede ser sufrido tanto por particulares como por empresas. Es por ello que parece coherente establecer determinadas normas en relación con la información que se recopila, así como el lugar y protección que se da a la misma. El mundo de la informática se encuentra en constante movimiento e innovación lo que supone un riesgo aun mayor puesto que habrá de adaptarse con rapidez a los nuevos peligros que puedan surgir. Además, en el ámbito del *Big Data* parece coherente establecer límites respecto a la cantidad de información que se recopile, o al menos ser proporcional en el sentido de brindar una mayor seguridad a mayor sea la cantidad de información. Esto puede afectar también al tipo de información, y es que podrían comprometerse informaciones tales como historiales clínicos de pacientes lo que supondría un riesgo, ya no solo para la privacidad de las personas sino también para la salud.

[34]Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016
[35]RICHARDSON, R. Y NORTH, M.: "*Ransomware: Evolution, Mitigation and Prevention",* disponible en: https://digitalcommons.kennesaw.edu/cgi/viewcontent.cgi?article=5312&context=facpubs
[36]PEREZ, F.: *Ciberseguridad: Ransomware* disponible en: http://www.cantabriatic.com/ciberseguridad-ramsonware-parte-i/

3.- EVOLUCIÓN DE LA REGULACIÓN SOBRE EL *BIG DATA*:

En este apartado se presenta la legislación que guarda relación con el *Big Data*, principalmente, desde la perspectiva de la protección de datos. Centraré mi análisis en la legislación nacional y europea y por último haré hincapié en las condiciones generales de la contratación, así como en las condiciones de uso de las redes sociales que presentan gran importancia en esta materia.

En la actualidad, la persona afectada por el tratamiento de datos goza de una serie de derechos[37] que se han ido perfilando a través de los diferentes textos normativos aprobados hasta la actualidad. Estos derechos, entre otros, son:

- Derecho de acceso: consiste en tener conocimiento sobre si se están tratando o no los datos del interesado.
- Derecho de rectificación: consistente en la modificación de datos inexactos.
- Derecho al olvido: ante determinados supuestos cabe pedir la supresión de datos personales.
- Derecho a revocar el consentimiento ante el responsable del tratamiento.
- Derecho a la limitación en el uso de los datos.
- Derecho a impugnar cualquier decisión tomada sobre los datos obtenidos a través del procesamiento de datos.

3.1 Derecho a la protección de datos personales: Constitución Española y Carta de los Derechos Fundamentales de la UE

El Derecho a la protección de datos personales[38] emana directamente de nuestro texto constitucional, concretamente, del artículo 18 relativo al honor, intimidad y propia imagen. En el apartado número cuatro se alude a la idea de 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*

[37]Agencia Española de Protección de Datos, derecho y deberes, disponible en: https://www.aepd.es/es/derechos-y-deberes/conoce-tus-derechos
[38]Derecho Fundamental a la protección de datos de carácter personal, disponible en: https://datos.redomic.com/Archivos/GuiasUtiles/G33.pdf

de sus derechos". Siendo el Tribunal Constitucional, en la Sentencia 292/2000[39], el que concretó que el derecho a la protección de datos es un derecho fundamental y, además, establece que los titulares tendrán la potestad de disposición sobre sus datos, es decir, podrán cederlos a través del consentimiento.

En cuanto a su alcance, el TC considera que al referirnos a la protección de datos personales se alude a "*cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual, …, sino los datos de carácter personal. cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos".* Con esto el Tribunal establece que aquellos datos que los datos personales públicos, que pueden ser conocidos por cualquiera, también se encuentran bajo la protección de este derecho y bajo la facultad de disposición del titular. Por lo tanto, se entiende que la protección se extiende a los datos que identifiquen o permitan identificar a la persona, es decir, los datos que mediante su procesamiento puedan llevar a la elaboración de perfiles ideológicos, raciales, económicos o de cualquier índole. Si bien es cierto que existen otros datos[40], regulados por normas específicas, que no gozan de esta protección legalmente prevista. Existen normas específicas que regulan el uso de datos que por sus características son tratados con fines determinados, por ejemplo, el uso que se da a los datos procedentes de imágenes y sonidos obtenidos por las Fuerzas y Cuerpos de Seguridad en el desarrollo de sus funciones.

Cabe resaltar que el derecho fundamental a la protección de datos permite a las personas controlar el uso que se haga de estos datos, así como disponer y decidir sobre los mismos. Es decir, se establecen una serie de garantías con objeto de conocer el tratamiento que se da a los datos personales procesados y, de ser necesario, el titular goza de un derecho de modificación o supresión de esa información.

Con objeto de garantizar y proteger el Derecho Fundamental a la protección de datos, reconocido en el 18.4 CE, se aprueba la Ley Orgánica 15/1999[41] así como del Reglamento 1720/2007[42] que la desarrolla. Aspecto relevante de esta LO es la designación de la Agencia Española de Protección de datos como órgano destinado a la tutela del derecho a la protección de datos. La legislación española se aplicará cuando el procesamiento de los datos

[39]SENTENCIA 292/2000, de 30 de noviembre, Fundamento Jurídico 5 (consideración como derecho fundamental) y 6 (delimita el objeto de protección)
[40]GIL, E.: "*Big data, privacidad y protección de datos*" ed.: AEPD y AEBOE, Madrid, 2016, pp. 50
[41]Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal
[42]Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal

lo lleve a cabo un sujeto que se encuentre desarrollando actividades propias de su negocio en territorio español. También habrá que atender a las normas de Derecho Internacional Público para determinar si resultan de aplicación las normas nacionales en supuestos en que los responsables del tratamiento de datos se encuentren fuera del territorio español.

Por otra parte, en el marco legislativo de la Unión Europea[43], el derecho a la protección de los datos personales también encuentra amparo. Se reconoce este derecho, así como la obligación de promover y garantizar su protección a todos los Estados miembros. Además, la UE precisa que será necesaria una autoridad independiente que garantice y tutele el derecho a la protección de datos.

Encontramos el reconocimiento de este derecho en el Tratado de Funcionamiento de la Unión Europea[44], concretamente en el artículo 16, antiguo artículo 286 TCE[45], se reconoce el derecho a la protección de los datos de carácter personal a toda persona, independientemente de su nacionalidad. Así mismo, en el apartado número 2, se establece que serán el Parlamento Europeo y el Consejo los que se encarguen de la elaboración de leyes relativas a la protección de las personas en materia de tratamiento de datos de carácter personal. Además, encomienda a los Estados miembros la labor de protección del derecho de la Unión, específicamente, en lo relativo a este derecho de protección de datos, así como el control de estas normas a través de una autoridad independiente. En el artículo 16 también se hace una referencia al artículo 39 del Tratado de la UE[46] en el que se incide en la idea de que el Consejo adoptará una decisión que fije las normas sobre protección de datos e, igualmente, incide en la necesidad de una autoridad independiente que garantice el cumplimiento de dichas normas.

El derecho a la protección de datos se encuentra protegido por el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea[47] que reconoce el derecho a la protección de datos a todas las personas, independientemente de su nacionalidad. Asimismo, en el apartado número 2, se hace referencia a la forma de procesar los datos, siendo el tratamiento "*de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley*". En este mismo artículo se menciona también la garantía de acceso a los datos recopilados, así como la modificación y supresión

[43]GIL, E.: "*Big data, privacidad y protección de datos*" ed.: AEPD y AEBOE, Madrid, 2016, pp. 49
[44]Tratado de Funcionamiento de la Unión Europea del 26/10/2012
[45]Tratado Constitutivo de la Comunidad Europea de 12 de junio de 1985
[46]Tratado de la Unión Europea, versión consolidada del 30.3.2010
[47]Carta de los Derechos Fundamentales de la Unión Europea de 18 de diciembre del 2000

de los mismos. Por último, en su aparatado tercero, se somete el respeto de estas normas al control de una autoridad independiente en cada Estado miembro.

En conclusión, nos encontramos con una herramienta como es el *Big Data* que se centra en la captación de datos de diferentes fuentes y, respecto a los datos relativos a la persona, estos gozan de alta protección. Estas garantías residen en la consideración del derecho a la protección de los datos personales como derecho fundamental, con las protecciones que ello conlleva. En el proceso del *Big Data,* por tanto, habrá que atender a la fuente de los datos para verificar que no se está produciendo una violación de este derecho en su captación y, además, tendrá que verificarse que los métodos de procesamiento se ajustan a derecho, tratando la información de forma leal, para fines concretos y sobre la base del consentimiento.

3.2 La Directiva 95/46/CE

En el marco de la Unión Europea se aprueba la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995, que fue reemplazada por el Reglamento General de Protección de Datos. Esta directiva se centraba en la materia de protección de datos personales, tratando de unificar la protección en los distintos Estados miembros. En cuanto a su necesidad, esta se basaba, además de en la unificación de legislación, en la necesidad de crear un espacio común que permitiera el intercambio de datos.

El principal objetivo[48] de esta directiva era garantizar el equilibrio entre el alto nivel de protección que se brinda a la vida privada de las personas y la circulación de datos personales dentro del territorio de la Unión. Las principales directrices de la directiva son, por un lado, el establecimiento de protocolos de control de los procedimientos de captación y procesamiento de datos, estableciendo sus límites. Por otra parte, se encomienda a los Estados miembros la creación de órganos independientes con la labor de supervisar las actividades en que se produzca algún tratamiento de datos.

La directiva centra su objeto en el tratamiento de datos, tratando de garantizar la protección de los derechos y libertades de los individuos, estableciendo pautas para asegurar que el tratamiento sea lícito y leal. Uno de los pilares en que ha de respaldarse el tratamiento

[48]EUR-Lex home: "*Summaries of EU Legislation*", disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=LEGISSUM%3Al14012

de datos, para ser considerado licito, es en la obtención inequívoca del consentimiento. Por ello, el uso de la información ha de ser acorde al fin con que se recogió la información, sin incurrir en excesos. Además, la directiva incluye ciertos derechos, como son el derecho de acceso y de oposición, que pueden ser ejercitados contra el responsable del tratamiento de datos.

La presente directiva además tiene en cuenta las "*Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales*"[49] a través de las cuales se establecen una serie de principios básicos que son, entre otros, la limitación en la recogida de datos, la especificación del propósito de su uso, la necesidad del consentimiento para la captación y tratamiento, transparencia en cuanto a conocer quien emplea los datos, etc.

A raíz de esta directiva se produce la iniciativa legislativa nacional por los distintos Estados miembros de la UE para transponer los criterios de esta directiva a la legislación nacional, suceso que se produce en España con la promulgación de la LO 15/1999.

3.3 Ley Orgánica 15/1999, de 13 de diciembre de protección de datos de carácter personal con base en la Directiva 95/46/CE

La Ley Orgánica 15/1999, de 13 de diciembre, sobre Protección de Datos de Carácter Personal entró en vigor el 14 de enero del 2000 y fue derogada por la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

La LO 15/1999 se elabora con la intención de desarrollar el artículo 18 de la Constitución. En su articulado se recoge la finalidad de la norma que será "*garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar*". La necesidad de la elaboración de esta norma surge con la Directiva 95/46/CE[50] que trataba de garantizar la protección de la intimidad de los individuos, concretamente en lo que respecta al tratamiento de los datos personales. En el articulado de la directiva se plantean una serie de límites,

[49]Organización para la Cooperación y el Desarrollo Económicos "*OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*", disponible en: https://www.oecd.org/sti/ieconomy/15590267.pdf

[50]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

respecto al tratamiento de datos, que han de tomarse en cuenta por los Estados miembros para garantizar los derechos de los individuos. Además, se brinda la potestad de desarrollar legislativamente tales limites argumentando posibles excepciones, siempre y cuando, sean relativas a los supuestos previstos en el artículo 13 de la directiva, asuntos como defensa, seguridad pública, seguridad estatal, etc.

En cuanto al ámbito de aplicación de la norma, este se extenderá a los "*datos de carácter personal*", es decir, información relativa a personas físicas identificadas o identificables que sean susceptibles de tratamiento. Respecto a los supuestos que abarca, se extenderán a situaciones en que el tratamiento se realice en territorio español y, también, las situaciones fuera del territorio nacional en que el Derecho Internacional Público lo determine. Así mismo, se establecen determinadas excepciones como son las relativas a datos estadísticos, electorales, que afecten al régimen del personal de las Fuerzas Armadas, etc.

En esta norma se establecen determinados criterios en relación con la calidad de los datos, la recopilación de datos tendrá que verificar que la información tratada atiende a los criterios de veracidad y guarda relación con el fin marcado en su obtención. El encargado para la captación de datos, para poder obtenerlos, necesita el consentimiento de la persona que cede los datos, y, este consentimiento, habrá de ser "*inequívoco"* y siempre en un contexto explícito y transparente. Para garantizar que el consentimiento no se vicie y evitar medios fraudulentos de obtención de los datos, habrá que informar de forma "*expresa, precisa e inequívoca"* de la intención de captar y tratar esos datos para unos determinados fines. La posesión de los datos no legitima su uso indiscriminado, habrá que atender al consentimiento de la persona que los cedió y emplearlos dentro de los limites en que se hizo esa cesión. Respecto al uso de los datos por un tercero, habiendo sido cedidos por quien los captó, tendrán que emplearse para los fines para los que fueron obtenidos y, como regla general, será necesario el consentimiento del interesado para la cesión. Esta norma garantiza el derecho de acceso a los datos cedidos, así como los derechos de rectificación y cancelación.

En cuanto a la tutela de los derechos reconocidos en esta norma, se encarga a la tutela la Agencia de Protección de Datos esta función. La APD es un órgano independiente, con autonomía presupuestaria y funcional, creada en 1992. En cuanto a su actuación, desarrolla funciones de "control" por lo establecido por el Reglamento General de Protección de

Datos[51] que obligaba a los Estados miembros a establecer un órgano para el control y aplicación de la normativa sobre tratamiento y circulación de datos personales en la Unión.

Nos encontramos ante una norma que viene a trasponer las directrices marcadas por la Unión Europea, así como a desarrollar los derechos recogidos en nuestra constitución. Se trata, por tanto, de una norma acorde a su tiempo, que cubría los supuestos que se planteaban, pero que, con el desarrollo tecnológico y la globalización, queda obsoleta ante los nuevos retos que se plantean y pone de relieve la necesidad de una modernización de la normativa.

3.4 Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo

Ante la imperiosa necesidad de sustituir el antiguo marco normativo de la Unión se aprueba el *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos*. Este Reglamento resulta de aplicación directa para todos los Estados miembros, sin necesidad de transposición, lo que supone la derogación de la Directiva 95/46/CE. La anterior directiva supuso varios problemas principalmente porque no fue transpuesta de igual forma en todos los Estados miembros, sino que se hizo de forma fragmentada y desigual. La fragmentación, junto a las diferentes normativas estatales, dio lugar a un panorama en el que existían grandes divergencias en cuanto al nivel de protección de los derechos y libertades de los individuos. Estas diferencias dieron lugar a numerosos impedimentos en la circulación de datos dentro de la Unión Europea y, con ello, la obstaculización de actividades económicas, dándose conductas contrarias al Derecho de la Competencia, que no podían ser abordadas por las autoridades europeas por las diferentes regulaciones nacionales. Estas circunstancias, junto al impacto de las nuevas tecnologías que crearon situaciones que superaban a las legislaciones previas, hicieron resaltar la necesidad de una reforma legislativa a nivel europeo. Con este Reglamento se trata de armonizar la normativa en materia de protección de datos dentro del territorio de la UE. Es interesante que la regulación de esta materia se realizara de esta forma puesto que con la aprobación del Reglamento se garantiza la uniformidad normativa, por su aplicabilidad directa, así como la

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

consonancia en la interpretación de la norma por los Estados miembros. Junto con el mencionado interés en la unificación legislativa, este Reglamento realiza una tarea de adaptación de la normativa a las nuevas circunstancias creadas por el avance tecnológico y, además, incide en ampliar la protección de datos con el objetivo de garantizar ese derecho fundamental. Esta tarea se centra en ampliar el control que puedan tener los afectados por el tratamiento de datos a través de técnicas que fomentan la transparencia.

Respecto a las novedades que plantea el Reglamento[52], una de ellas, es la necesidad de elaborar un registro por parte de los responsables tratamiento de datos con el fin de tener un control de sus actividades. Este registro habrá de estar actualizado y disponible para permitir el acceso a los distintos órganos independientes de control de cada Estado y con ello garantizar el control de las actividades de procesamiento. En cuanto a las garantías, se refuerzan las medidas para la obtención del consentimiento de los afectados, que tendrá que obtenerse a través de la libre manifestación de los individuos. La voluntad del consentimiento tendrá que referirse a un supuesto específico y previamente informado de forma inequívoca. Todas las medidas van encaminadas a garantizar la obtención y el uso de los datos de una forma leal y transparente. Las personas encargadas del tratamiento de datos, en el afán de garantizar la transparencia, tendrán el deber de informar, en la medida de lo posible, sobre la cantidad de datos recopilados, así como el plazo por el que van a ser empleados esos datos. Así mismo, debe facilitarse el trabajo a los delegados de protección de datos y favorecer la comunicación con las personas que han cedido los datos.

En cuanto a los derechos reconocidos o extendidos, respecto a la normativa anterior, nos encontramos con la inclusión del derecho de supresión. El derecho de supresión, también conocido como el derecho al olvido, aparece en el artículo 17 del Reglamento de tal forma que la persona cuya información es tratada puede "*obtener, sin dilación indebida, la supresión de los datos personales que le conciernan*" en las circunstancias que se plantean en este artículo. Por otra parte, aparece el derecho de portabilidad de datos, en el artículo 20, que permite al interesado recibir los datos procesados por un responsable de tratamiento, que tendrá que colaborar traspasando los datos, para ceder esa información a otro responsable de tratamiento. Otro punto novedoso es el incluido en el artículo 22 del Reglamento que trata las "*Decisiones individuales automatizadas"* entre las que se incluye el "*profiling*"[53], entendido como

[52]Información sobre el *Reglamento general de protección de datos*, disponible en: https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_es.htm

[53]Artículo 4.4 del REGLAMENTO (UE) 2016/679 Reglamento General de Protección de Datos

elaboración de perfiles. Nos encontramos con que el Reglamento, en el apartado primero de este artículo, permite a los interesados determinar si quieren que sus datos sean objeto de un procedimiento por el que se elaboren perfiles.

Otro de los aspectos optimizados por el Reglamento aparece en la sección 4, en lo relativo a los delegados de protección de datos. En esta sección, en el artículo 37, se establece que serán el responsable y el encargado del tratamiento quienes designarán un delegado de protección de datos en el caso de que el tratamiento lo realice un organismo público, excepto en el caso de los tribunales. Así mismo, si las actividades principales del responsable o del encargado consistieran en operaciones de tratamiento que requieran una supervisión habitual y sistemática será necesaria la designación de un delegado de protección de datos.

El Reglamento incluye la posibilidad de establecer un régimen de sanciones a los Estados en los supuestos no previstos en el artículo 83 del Reglamento. En este último artículo se fijan las sanciones administrativas pudiendo ir desde los 10 millones de euros hasta los 20 millones de euros o afectando desde el 2% del al 4% como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optando por la medida más gravosa. Dependiendo de la infracción se recurrirá a un régimen u otro, si la situación atiende a un supuesto de incumplimiento del nombramiento del delegado de protección de datos o si afecta a los derechos o disposiciones del Reglamento.

En conclusión, el Reglamento otorga un mayor control a los ciudadanos europeos sobre su información privada, partiendo de las facilidades y garantías que se brinda a las personas. Considero que la inclusión de los derechos de olvido, portabilidad de datos y decisión sobre la elaboración de perfiles aportan seguridad jurídica. Además, se facilita de manera enorme la obtención de información sobre el procesamiento de datos, pudiendo solicitar información sobre el alcance del tratamiento de datos, conociendo en qué forma y en qué plazo se ha empleado esa información. Para conseguir este grado de control y transparencia, con el fin de acreditar el cumplimiento del Reglamento, será necesaria la colaboración del responsable de tratamiento que tendrá que seguir las directrices marcadas para no vulnerar los derechos de los ciudadanos. Considero que las medidas relativas a la elaboración de un registro y su actualización son de vital importancia para que pueda ser controlado el proceso de tratamiento de datos y, por supuesto, el hecho de facilitar el acceso a ese registro es otro punto decisivo. Por último, resaltar que el hecho de emplear la figura del Reglamento era algo necesario para establecer un marco común en el territorio europeo, siendo de obligado cumplimiento y aplicación en los Estados miembros.

3.5 Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales

En España, a raíz de la promulgación del Reglamento General de Protección de Datos, se aprueba el Real Decreto-ley 5/2018, de 27 de julio sobre "*medidas urgentes para la adaptación del Derecho español a la normativa de la Unión Europea en materia de protección de datos*" que supuso la adaptación de nuestro ordenamiento a la normativa europea. Este Real Decreto venía a cubrir aspectos que el Reglamento dejaba en manos de los Estados hasta la promulgación de una Ley Orgánica que adaptase nuestro ordenamiento a las exigencias que marca el Reglamento.

El día 7 de diciembre de 2018 entra en vigor la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, que viene a derogar el Real Decreto-ley 5/2018. Con esta ley se configura el actual marco legislativo relativo a la protección de datos y, además, se establece en el Título X garantías de los derechos digitales.

En cuanto al objetivo de esta LO viene a ser, por un lado, la adaptación del ordenamiento jurídico español al Reglamento (UE) 2016/679 y garantizar el derecho fundamental la protección de datos y, por otra parte, garantizar los derechos digitales conforme a la Constitución. Es importante resaltar que esta ley viene a ser el marco general de regulación pero que ciertos datos, por sus características, podrán ser tratados con arreglo a normas específicas. Esta ley incluye otro aspecto relevante, en el artículo 3, relativo a la cesión de los derechos de las personas fallecidas a las personas vinculadas al interesado, familiares o parejas de hecho. Las personas vinculadas podrán solicitar el acceso a los datos personales del fallecido y, en su caso, su rectificación o supresión.

Esta ley establece un marco de protección de datos, en los artículos 4 y siguientes, recogiendo la necesidad de confidencialidad, de todos los sujetos involucrados en el tratamiento de datos, así como la garantía de exactitud de los datos obtenidos. El tratamiento de datos habrá de basarse en el consentimiento, entendido como la "*manifestación de voluntad libre, específica, informada e inequívoca"*. Todo ello sin perjuicio de que ciertos datos, por sus características o por las características del tratamiento, se obtengan sin consentimiento por responder a fines legales o de interés público. Además, el Reglamento regula el consentimiento de los menores de edad que será aceptado, como regla general, cuando el menor sea mayor de 14 años o cuando se autorice por el titular de la patria potestad.

Encontramos el Titulo III relativo a los derechos de las personas que viene a marcar la idea de transparencia e información plasmada en el Reglamento General de Protección de datos. El interesado tendrá acceso a la información básica que no será otra que la identidad del responsable del tratamiento, la finalidad del tratamiento y el ejercicio de los derechos establecidos en el Reglamento. En este mismo título, en el capítulo II, se encuentran las directrices relativas al ejercicio de los derechos.

En los sucesivos artículos se establecen las normas relativas al tratamiento de datos a través de ciertos procedimientos específicos, así como la regulación del responsable y encargado del tratamiento.

En el Titulo VII se regula lo relativo a las autoridades de protección de datos, encomendando a la Agencia Española de Protección de Datos, como autoridad independiente, la función de tutelar el derecho a la protección de datos y garantizar el cumplimiento de la LO y el Reglamento General de Protección de Datos. Esta ley también habilita la creación de órganos autonómicos que desarrollen estas funciones.

Respecto a la Agencia Española de Protección de Datos (AEPD) es un órgano independiente encargado de garantizar el cumplimiento de la normativa relativa a la protección de datos. Además de las potestades relativas a la investigación y auditoria preventiva, la AEPD ostenta la potestad sancionadora. Por tanto, sus funciones se centrarán en el análisis del procedimiento mediante el cual se traten los datos para detectar posibles irregularidades y determinar las medidas correctoras oportunas. Ejerce además una función de auxilio a los afectados por el procesamiento de datos, atendiendo las reclamaciones e investigando los hechos. Así mismo, la AEPD participa en los procedimientos legislativos y reglamentarios en materia de protección de datos en calidad de asesor.

Por último, la ley incluye un título novedoso relativo a la "Garantía de los derechos digitales" con el fin de garantizar la aplicabilidad en Internet de los derechos y libertades recogidos en la Constitución y en los Tratados y Convenios Internacionales. Así mismo encomienda a los prestadores de servicios de internet la colaboración para garantizar su aplicación. Por otra parte, se reconocen nuevos derechos relativos al acceso a Internet, a la seguridad digital, derecho al olvido, etc.

A modo de resumen, considero que la consagración en una disposición legal orgánica de los derechos "ARCO", derecho de Acceso, Rectificación, Cancelación y Oposición, junto con la ampliación de derechos prevista en la ley, relativos a la supresión y portabilidad de los

datos supone otorgar seguridad jurídica a nuestro ordenamiento. Así mismo, considero relevante el hecho de que se incluya un título especifico que prevea la regulación de derechos digitales, basado en la necesidad de ampliar la protección al ámbito tecnológico, principalmente Internet, para cubrir posibles situaciones que no encuentren cabida dentro de nuestro ordenamiento jurídico.

3.6 Las condiciones generales

Uno de los aspectos de mayor importancia en lo relativo a *Big Data* y al flujo de datos reside en la forma en que se obtiene la información. Es frecuente que, tanto empresas como redes sociales, establezcan a través de "contratos" y "condiciones y términos de uso" cláusulas en las que autorizamos la captación y procesamiento de cierta información. A través de la aceptación de las condiciones de privacidad[54] que encontramos en los contratos estamos otorgando nuestro consentimiento para el procesamiento de datos.

En múltiples ocasiones estas empresas recurren a contratos de adhesión, entendido como modalidad contractual cuyo elemento definidor es la unilateralidad del contenido contractual, así como la falta de capacidad fáctica por parte del adherente en lo que respecta a variar el contenido[55]. Llegado este punto, cable plantearse qué normativa resultará de aplicación, siendo la normativa de defensa de consumidores aplicable en ciertos supuestos, concretamente el texto refundido[56] de la a Ley General para la Defensa de los Consumidores y Usuarios. Esta norma tiene por objeto garantizar la protección de los consumidores y usuarios en las relaciones con empresarios. Uno de los derechos que se conceden a los consumidores y usuarios es el previsto en el artículo 8 b) relativo a "*la protección de sus legítimos intereses económicos y sociales; en particular frente a las prácticas comerciales desleales y la inclusión de cláusulas abusivas en los contrato*s". Para garantizar esta protección el artículo 60 establece la obligación del empresario de facilitar de forma clara y comprensible la información de carácter sustancial. Se trata de un requisito previo a la vinculación que exige la exposición de las condiciones del contrato de forma veraz y suficiente. Además, según el artículo 94, en los

[54]MEGÍAS, J.: "*Construcción de redes sociales garantes de la privacidad*" en LOMBARTE/MARTÍNEZ (Cords): "*Derecho y redes sociales*", Thomson Reuters, Navarra, 2010, p. 73
[55]Sentencia Nº 297/2016 de 7 de diciembre de 2016, Juzgado de lo Mercantil, Barcelona
[56]Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias

supuestos de contratación electrónica o a distancia se aplicará de forma supletoria la normativa de servicios de la sociedad de la información y de comercio electrónico.

El articulo 59.3 delimita el ámbito de aplicación de la LGDCU incluyendo también el sometimiento a la Ley 7/1998[57] los contratos, con consumidores y usuarios, que incorporen condiciones generales de la contratación. La ley sobre condiciones generales de la contratación establece una serie de requisitos en relación con la redacción de las cláusulas que deberá atender a los criterios de transparencia, claridad, concreción y sencillez. Las condiciones que no se ajusten a estos criterios podrán ser consideradas nulas. Además, según el artículo 8 se considerarán nulas de pleno derecho las condiciones que contradigan lo dispuesto en esta Ley o en cualquier otra norma imperativa o prohibitiva.

Parece obvio que cada vez más empresas están incluyendo cláusulas en las que se incluyen autorizaciones para la obtención de ciertos datos y su posterior procesamiento o cesión. Es por ello por lo que al ofrecer un producto o servicio debemos de prestar atención al método por el cual obtenemos la prestación o nos vinculamos al servicio y, por supuesto, observar si se incluyen clausulas relativas a nuestros datos y privacidad. Como ya se ha expuesto, estas cláusulas habrán de aparecer de forma clara y detalladas, incluyendo no solo la cuestión de captar información si no también la forma de tratamiento.

Por ejemplo, al vincularse al servicio de la red social "*Twitter*" se aceptan una serie de cláusulas que van desde los datos personales del usuario: nombre, apellidos, residencia, fecha de nacimiento, etc. hasta una autorización a recopilar información sobre nuestra ubicación y dirección IP.

En conclusión, considero que el riesgo que supone que estas cláusulas no atiendan a los criterios de claridad y transparencia pueden generar problemas. Estos peligros se presentan cuando las personas ceden datos sin conocimiento poniendo en riesgo su privacidad y pudiendo afectar en algunos casos a la vida privada, el honor y a la intimidad. La plataforma "*Facebook*", por ejemplo, recopilaba datos personales relativos situación sentimental, religión o ideales políticos que quedan a disposición de las distintas empresas, y esto supone grandes riesgos. Por ello considero que han de llevarse a cabo políticas de transparencia y concienciación para que el avance del uso de la tecnología del *Big Data* no suponga la inclusión de cláusulas que no se ajusten a la normativa y que puedan llevar a la vulneración de derechos fundamentales.

[57]Ley 7/1998, de 13 de abril, sobre condiciones generales de la contratación

4.- VALORACIÓN DEL USO DE LA INFORMACIÓN RECOPILADA DESDE LA PERSPECTIVA DE LA ÉTICA

4.1 ¿La gratuidad de los servicios legitima la recopilación y uso de los datos?

Una de las cuestiones que se ha planteado a raíz del fenómeno del *Big Data* es la relativa al coste de obtención de la información[58]. Es un hecho que la captación de datos supone un proceso sumamente simple y, por tanto, con un coste bajo o nulo. El proceso de obtención de datos puede hacerse de diversas formas, pero los métodos más frecuentes son el recurrir a datos públicos u obtener el consentimiento de los afectados aprovechando otras actividades comerciales. De esta forma, se consigue el acceso a los datos de una forma simple y rápida y con un margen de beneficio muy alto. Por el contrario, los cedentes no ven ningún rendimiento en esta cesión. El negocio a partir del cual se obtiene el consentimiento es diverso, aunque es bastante recurrente la idea de ofrecer un servicio, aparentemente gratuito, a cambio del consentimiento para tratar los datos del usuario. Algunas de estas formas son el acceso a información a cambio de la instalación de "*apps gratuitas*", a través de la suscripción a un catálogo online, permitiendo la geolocalización en redes sociales, etc.

De lo anteriormente expuesto podemos considerar que existen distintos tipos de datos en función de la fuente de obtención[59], pudiendo diferenciarse: datos voluntariamente cedidos, datos observados sin que el usuario los facilite y, por último, los datos obtenidos a través del procesamiento de otros datos, los denominados datos inferidos.

En la actualidad, una de las necesidades sociales más extendida es la de "estar conectados" lo que conlleva emplear la tecnología y los servicios digitales. El uso de los servicios digitales supone aceptar la cesión de cierta información y, con esta cesión, estamos permitiendo que una empresa tenga acceso a datos relativos a nuestra privacidad pudiendo verse comprometidos nuestros derechos. Por ejemplo, el simple hecho de realizar búsquedas a través de un buscador como es Google, considerado como un servicio "gratuito", supone la cesión de datos como nuestro historial de búsqueda en el que se asociará a nuestra persona ciertos parámetros en función de nuestra actividad y esto será empleado por Google de forma comercial o a través de la cesión a terceros esa información. Por tanto, un servicio que

[58]MARTINEZ, L./SANCHO, M.: "*El nuevo concepto de onerosidad en el mercado digital. ¿Realmente es gratis la App?"* en InDret nº 1, 2018, pp. 14 y ss.
[59]HILDEBRANDT, M.: "*Esclavos de los macrodatos. ¿O no?*" en Revista de Internet, Derecho y política, nº 17, 2013, pp. 13

aparentemente se perfila como gratuito, en realidad, no lo es, puesto que procesa nuestros datos y los comercializa a cambio de prestar el servicio.

Respecto a las redes sociales[60], a través del registro, aceptamos ciertas cesiones de datos relativos a nuestro ámbito personal como son la edad, nombre, número de teléfono, etc. y esa información es captada y almacenada. Las redes sociales, que ofrecen en principio un servicio gratuito, están recopilando información que más tarde será utilizada para generar un beneficio directamente con su uso o a través de la cesión. Nos encontramos, por tanto, con que la entrega de datos personales supone una contraprestación por el uso de un servicio digital. El problema reside principalmente en que los datos no se plantean en ninguna legislación como un "producto" al que se le pueda dar un uso comercial, pero, sin duda, es lo que se está produciendo. Junto al riesgo que supone el consentimiento para el tratamiento de datos, existe otro problema relativo a los datos que volcamos en las redes y son de acceso público. Es una realidad que las empresas tienen acceso a las redes sociales y a la información que en ellas publicamos y que, a través de la Inteligencia Artificial y el *Big Data*, pueden obtener ganancias aprovechando que los usuarios no tienen información sobre el procesamiento de datos y tampoco existe un interés en conocer el uso que se va a dar a los mismos, simplemente, se asume esa cesión de información para obtener un servicio. Esto supone una doble exposición de nuestra privacidad, por un lado, a través de la información tratada por la red social y, por otra parte, la información que otras empresas pueden recopilar de los perfiles y publicaciones de las distintas redes sociales.

Los datos son en la actualidad el "nuevo petróleo" y las empresas conocedoras del gran valor de la información están desarrollando técnicas de recopilación y procesamiento de datos para maximizar sus beneficios que en ocasiones suponen verdaderas expropiaciones de privacidad. Es comprensible que, asentándose como uno de los pilares de la economía futura, las empresas, tratando de adaptarse al mundo digital, lleven a cabo políticas de potenciación relativas al *Big Data*. El RGPD trata de otorgar a los ciudadanos protección y control sobre sus datos, pero es una realidad que los ciudadanos no muestran excesiva preocupación[61] sobre la política de privacidad de las empresas. Estas empresas, en contraposición a la preocupación ciudadana, centran todos sus intereses en captar la mayor cantidad de datos, lo que supone poner en peligro la privacidad de las personas. La necesidad

[60]ORBE, A.: "*Ética y Big Data*", disponible en: https://telos.fundaciontelefonica.com/etica-y-big-data/

[61]MERINO GOMEZ, G.: "*Nuevos desafíos en torno al Big Data*" en Revista de Derecho y Genoma Humano, núm. extraordinario, 2019, pp. 37-54

de que el consentimiento para el tratamiento de datos sea válido debe concretarse a través de los requisitos de especificidad, libertad e información. El cumplimiento de estas características supone autorizar el tratamiento de datos en contra de la prohibición generalizada de datos[62]. El problema reside en que el consentimiento en una relación como la que se presenta entre las personas y las empresas puede no ser un instrumento adecuado para regular la captación de datos. En esta relación, las personas, desconocedoras en muchos casos de las consecuencias, otorgan ese consentimiento y las empresas proceden a procesar sus datos en ocasiones incurriendo en tratamientos de datos excesivos. El tratamiento debería ser adecuado y no excesivo al fin por el cual se obtuvieron los datos, pero algunas empresas centrándose en la indeterminación o generalización del consentimiento extienden el procesamiento a datos que no deberían de ser tratados. Concretamente en España, la AEPD, sancionó a WhatsApp y Facebook[63] por llevar a cabo un procesamiento de datos no acorde a la legislación, captando en datos sin haber obtenido un consentimiento expreso, sino que se basaban en el consentimiento general otorgado al registrarte en el servicio.

El hecho de que la tecnología sea capaz de captar y procesar la información de una forma tan veloz, junto con la fragmentación legislativa, posibilita la aparición de un negocio muy rentable. Estos negocios se basan en una obtención gratuita de la información, a través de la oferta de servicios sin coste, lo que supone un gran riesgo para la privacidad de las personas. Los intereses en juego son la privacidad de las personas y los derechos relativos a la intimidad. No parece coherente que se pueda ofertar un servicio gratuito, cuando en realidad es una fuente de información empleada para hacer negocio. La realidad es que no estamos ante consumidores pasivos, nos encontramos con que las personas que usan determinados servicios en línea se han convertido en verdaderos proveedores de datos que no ven beneficios de la comercialización de sus datos. Es evidente que el usuario al emplear determinados servicios digitales obtiene de forma gratuita aquello que necesita, lo que supone un beneficio para el usuario y un coste para quien ofrece ese servicio. El problema se encuentra en el uso de determinados servicios en los que se aceptan condiciones de uso y servicio relativas a la captación de datos durante el uso del servicio y posteriormente. Esto queda plasmado perfectamente en el uso de aplicaciones de Google como la aplicación "*Google Maps*" la cual nos ofrece un servicio de GPS gratuito pero que recopila información sobre nuestra ubicación y la relaciona con comercios cercanos. Además de recopilar datos

[62]MORTE FERRER, R.: *"¿Protección de datos/privacidad en la época del Big Data, IoT, wearables…? Sí, más que nunca*" en Revista Dilemata, num. 24, 2017, pp. 220 y ss.
[63]Sanción de la AEPD a Facebook y Whatsapp disponible en: https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/la-aepd-sanciona-whatsapp-y-facebook-por-ceder-y-tratar

durante el uso de la aplicación, Google lleva a cabo una recopilación de datos[64] relativos a la ubicación (mediante GPS, dirección IP, etc.) de los usuarios cuando estos no están empleando sus servicios. Por lo tanto, el problema reside en que para emplear determinadas aplicaciones se han de conceder ciertos permisos que se extenderán más allá del momento en que usemos ese servicio. Por tanto, habrá que atender a la relación que existe entre el uso que se da a la aplicación y el coste que supone a la empresa y el beneficio que esta obtiene. Es una realidad que los usuarios emplean estos servicios generalmente de forma puntual y la empresa obtiene la potestad de captar y procesar datos de forma continuada obteniendo un lucro prolongado de una actividad ofertada como gratuita.

A raíz del análisis de esta cuestión surge la duda de si será válido el consentimiento otorgado al registrarnos en una red social, aceptando el tratamiento generalizado[65] de nuestros datos y no para un fin concreto. El consentimiento para el tratamiento de datos, como bien establecen las distintas normativas analizadas en este trabajo, plantea la especialidad de ser necesario su otorgamiento para un fin determinado, es decir, cuando se captan datos es necesario especificar que uso se va a dar a los mismos. Las redes sociales no indican con precisión que nuestros datos vayan a ser empleados como producto para obtener beneficio con su cesión o tratamiento. Estas generalidades incluidas en los términos y condiciones de uso son clausulas genéricas y abstractas que hacen que el usuario no sea consciente de su compromiso a través de la aceptación. Asimismo, estas cláusulas pueden ser consideradas nulas por no ser claras y concretas, siguiendo las exigencias de transparencia del RGPD.

Otro de los frentes que se abre es el de la responsabilidad penal de los gestores de redes sociales asociada a la información que aparece en las redes de personas que no son usuarias del servicio. La realidad es que en una sociedad tan conectada multitud de información fluye por las redes, pudiendo generar información a través de fotos, comentarios, perfiles relacionados, etc. sobre personas que no emplean servicios digitales. Esta brecha en la privacidad supone que, sin haber aceptado ninguna cláusula relativa al tratamiento de datos, las empresas pueden acceder a nuestra información a través de los perfiles de nuestros familiares y amigos, así como de nuestro centro de trabajo o estudio. El tratamiento que se hace sobre esta información supone una injerencia en los derechos

[64]Política de Privacidad de Google: Información recopilada disponible en: https://policies.google.com/privacy?hl=es

[65]PICCOTI, L.: "*Los derechos fundamentales en el uso y abuso de las redes sociales en Italia: aspectos penales*" en Revista de Internet, Derecho y Política, nº16, 2013, pp. 84

fundamentales relativos a los datos personales de los sujetos puesto que no han emitido consentimiento para ello y tampoco han sido informados del tratamiento.

Un posible ejemplo es el supuesto de publicaciones relativas a concesiones de ayudas que aparecen en los portales de las distintas administraciones. En estas publicaciones existen documentos que contienen información personal como puede ser el nombre completo junto el Documento Nacional de Identidad. Cualquier persona por medio de Internet puede tener acceso a los portales institucionales en los que hay documentos con información personal. Este tema fue abordado por el RGPD y la Ley 3/2018 limitando el acceso a la publicación a los interesados, no de forma general y publica, evitando asociar nombre y apellidos al DNI, todo esto para minimizar injerencias en los derechos fundamentales. A pesar de este desarrollo normativo siguen existiendo en la red documentos, previos a la ley, en los que se incluyen datos como el nombre, el DNI, residencia, centro de estudios, etc. Esta información puede obtenerse de manera fácil por las empresas suponiendo una vulneración de la privacidad de las personas.

Una de las posibles soluciones[66] para evitar este uso gratuito de datos en el que no aparece un consentimiento específico del afectado es la planteada por el RGPD a través del "*data protection by design*". Se trata de un intento de establecer un ámbito de protección del usuario en el que este tenga un control de sus datos y del uso que se da a los mismos. Se trata de potenciar el "consentimiento informado" entendido como la notificación a los usuarios del uso que se está dando o se va a dar a sus datos. El conocimiento de los datos publicados junto con la capacidad que tiene el interesado de modificación y supresión de los datos supondría una solución para estos supuestos de datos aun publicados en la ley.

En conclusión, parece evidente que en la actualidad los datos están monetizados y esto supone el origen de nuevos modelos de comercio. El crecimiento del interés por la captación de datos genera, a su vez, técnicas más peligrosas para la privacidad de los individuos. La gestión de datos personales es compleja por el desconocimiento acerca del valor de la información, pero parece prudente hacer partícipes de los beneficios a los proveedores de información. En cuanto a la forma de hacer esta distribución puede que no deba ser equitativa puesto que la información ha de ser procesada adecuadamente para obtener un beneficio y esto supone unos gastos de gestión. En cambio, sí que parece evidente que el derecho no puede dar rienda suelta a estos modelos de negocio que obtienen su

[66]HILDEBRANDT, M.: "*Esclavos de los macrodatos. ¿O no?"* en Revista de Internet, Derecho y política, nº 17, 2013, pp. 15

producto a través de servicios aparentemente gratuitos con el establecimiento de cláusulas abstractas alejadas de las directrices marcadas por la normativa vigente. Por ello, considero que una de las formas de advertir esta situación es eliminar el concepto de "gratuidad" asociado a determinados servicios que comercian con nuestros datos, para, de estar forma, concienciar a los usuarios de los intereses en juego.

4.2 El uso de inteligencia artificial y algoritmos para tratar los datos:

Uno de los aspectos más relevantes que se asocia a la tecnología[67] es la capacidad de realizar una tarea de forma correcta y rápida. Con la tecnología se dejan atrás las posibles intervenciones humanas y con ello el error humano. Parece evidente que se ha extendido la optimización de procesos con la automatización de la toma de decisiones a través del uso de la Inteligencia Artificial. Este hecho supone dejar en manos de la tecnología decisiones transcendentales que lejos de ser abordadas de forma imparcial están profundamente marcadas por los intereses plasmados en la creación de los algoritmos. Como veremos en los distintos apartados, la IA responde a la creación humana y trata de agilizar la toma de decisiones en las distintas materias. Hay que tener en cuenta que el uso de esta tecnología no elimina el factor humano ya que los parámetros para la toma de decisiones vienen impuestos por personas, pudiendo este componente humano estar influenciado por distintos intereses. Cada persona tiene sus preferencias y opiniones que se verán plasmados en las decisiones que tomaría cada individuo de forma aislada. El *Big Data* y la IA se alimentan de esas decisiones humanas y se emplean en este caso para poder elaborar un mecanismo de análisis y respuesta que ofrezca soluciones de una forma rápida pero no necesariamente justa.

Interesa desde el punto de vista del Derecho la idea de que cumplir con las exigencias legales puede resultar complicado si las decisiones se toman por medio de la IA. El derecho no se entiende como una disciplina matemática, sino que recurre a una valoración específica en cada supuesto teniendo en cuenta el contexto y las características específicas para poder dar una respuesta acorde a cada situación planteada.

[67]COLMENAREJO, R.: "*Ética aplicada a la gestión de datos masivos*" en Anales de la Cátedra Francisco Suárez, nº 52, 2018, pp 127

4.2.1 IA aplicada a la función judicial

Parece que la función judicial también ha sucumbido al avance de la tecnología apareciendo el uso de la Inteligencia Artificial en algunas fases y procesos judiciales. Una de las principales aplicaciones del *Big Data* dentro del ámbito judicial es la de predicción de resultados de los litigios. La empresa española *Legal Innovation*[68] ha desarrollado un software de predicción denominado "*Legal Data*" capaz de elaborar, a través del análisis de jurisprudencia, el resultado de un litigio futuro. El uso que se puede dar a esta aplicación difiere, pero es capaz de, ajustándose a ciertos parámetros, determinar el resultado de un litigio e, incluso, el tiempo aproximado para su resolución. Esta herramienta puede ser de gran utilidad para abogados y clientes pudiendo valorar el interés de plantear un litigio. Además, esta herramienta puede iniciar la creación de una herramienta de predicción empleada por los Tribunales para tomar decisiones en litigios de menor relevancia jurídica y con ello solventar las acumulaciones de asuntos en la justicia española.

En EEUU se ha extendido el uso de "*e-descovery*" dentro de la función judicial. En concreto, en el procedimiento civil americano encontramos una fase previa al juicio en la que se produce la recopilación de información que sea relevante para el litigo. El *Big Data* y la Inteligencia Artificial han aparecido en esta parte del "*discovery*" americano aportando facilidades a la hora de encontrar y presentar pruebas. En un mundo "electrónico" en que todos los datos se almacenan y procesan a través de la tecnología debe incluirse y regularse la obtención de medios de prueba a través de medios electrónicos. La información recopilada a través de estos medios se diferencia de otro tipo de pruebas por su intangibilidad y el gran volumen de datos. Es por ello que en EEUU se limita este "*discovery*" a través de las "*Federal Rules of Civil Procedure*".

También en Estados Unidos, en relación con el "*criminal rating*", se emplean ciertos instrumentos basados en *Big Data* e IA mediante los cuales se elaboran perfiles criminales, así como estadísticas sobre los resultados de los distintos litigios. Existen determinados programas como "*Correctional Offender Management Profiling for Alternative Sanctions*"[69]. "*COMPAS*" es un sistema que analiza las características de los delincuentes para evaluar la probabilidad de reincidencia. El sistema emplea un algoritmo que asocia determinados datos y circunstancias concretas a la probabilidad de reincidir. Se utiliza como sistema auxiliar para

[68]Servicio Legal Data disponible en: http://legal-innovation.com/legal-data-inteligencia-artificial-y-big-data-juridico/

[69]BRENNAN T. DIETERICH W.: "*Correctional Offender Management Profiles for Alternative Sanctions (COMPAS)*" en SINGH/KRONER/WORMITH (Cords): "*Recidivism Risk/Needs Assessment Tools*" ed. Wiley-Blackwell, Nueva Jersey, 2018, pp.49-75

la toma de decisiones judiciales como puede ser la conveniencia de conceder ventajas penitenciarias como la libertad condicional. La creación de un sistema como "*COMPAS*" responde a las aportaciones de distintos magistrados que a través de su criterio han creado un algoritmo que permite analizar las circunstancias particulares y llegar a tomar decisiones.

Los problemas que suponen emplear IA dentro de la función judicial estriban, por un lado, en que las decisiones son tomadas a través de predicciones algorítmicas lo que plantea problemas a la hora de justificar esas decisiones ante posibles recursos. Por otra parte, el problema que se aprecia en la toma de decisiones a través de IA es que el uso de este sistema no garantiza la imparcialidad. El sistema "*COMPAS*" se basa en los criterios de determinadas personas que tienen sus preferencias y opiniones y la creación de un algoritmo a través de los criterios personales de diferentes personas no garantiza que las decisiones finales sean imparciales. Las decisiones que se tomen por este sistema pueden resultar discriminatorias pese a haber sido tomadas por un algoritmo. Uno de los casos más sonados en EEUU es el asunto "*State v Loomis*"[70] en el que el Tribunal Supremo de Wisconsin decidió rechazar el recurso del señor Loomis que fue condenado en base a los criterios del sistema "COMPAS" y que, en su recurso, pedía tener acceso en profundidad al algoritmo que se empleó para tomar la decisión para poder elaborar así su defensa.

La Comisión Europea para la Eficiencia de la Justicia adoptó la Carta Europea[71] para el uso ético de la IA en la función judicial a través de la cual se pretende señalar determinados principios que habrán de respetarse. En un primer capítulo señalo los cinco principios que deben de guiar el uso de la IA. Estos principios son:

- Principio de respecto a los derechos fundamentales
- Principio de no discriminación
- Principio de calidad y seguridad
- Principio de transparencia, imparcialidad e igualdad
- Principio de "*under user control*"

Todos estos principios vienen a tener una función garantista para asegurar el respeto de las garantías judiciales y el debido proceso. Tanto los jueces, como el resto de las instituciones dentro de la función judicial, pueden acudir al uso de IA siempre y cuando

[70]881 N.W.2d 749 (2016) WI 68 STATE of Wisconsin, Plaintiff-Respondent, v. Eric L. LOOMIS, Defendant-Appellant.
[71]Carta Europea "*European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their environment*", Estrasburgo, 3-4 diciembre 2018

tengan en consideración que el uso de estos mecanismos tiene que respetar estos principios. Uno de los principales problemas que trata de evitar esta Carta Europea es la excesiva generalización de las decisiones judiciales, dando resultados iguales ante supuestos que tienen rasgos comunes, pero también diferentes. Es una realidad que la IA puede actuar dando facilidades y agilizando los trámites judiciales, pero esto no debe de comprometer la imparcialidad del sistema judicial y el análisis de los casos para evitar que se produzcan vulneraciones de derechos y discriminaciones. Por lo tanto, para poder emplear estos mecanismos, el uso de la IA debe ser implementado de manera que se puedan dar soluciones específicas a los diferentes litigios, evitando las decisiones judiciales estandarizadas.

Para concluir este apartado, parece evidente que existe una discriminación algorítmica[72] producida por el uso de IA en la función judicial. El riesgo parte desde la intromisión en la vida privada de los individuos, viendo afectada su intimidad y privacidad, y pudiendo afectar a las garantías procesales del individuo. Ciertamente el derecho de defensa es una de las garantías que más pueden verse comprometidas con la inclusión de IA en la función judicial. Parece evidente que una persona procesada que sea acusada mediante la decisión de un algoritmo no puede llevar a cabo una defensa adecuada puesto que no conoce en puridad las circunstancias y datos en las que se ha basado el algoritmo para tomar la decisión. Evaluando nuestros principios constitucionales y garantías procesales no parece posible concebir un proceso en el cual el acusado no tenga acceso a la base sobre la que se asienta su acusación o condena. De lo anteriormente expuesto considero que el emplear IA para obtener resultado de litigios, basando el resultado en ciertos datos conocidos, no puede venir a suprimir la intervención de una persona que valore concienzudamente las circunstancias específicas del caso. Parece, por tanto, que el uso de *Big Data* y de IA dentro de la función judicial puede poner en riesgo la independencia judicial del sistema, rompiendo también con la seguridad jurídica ya que el sistema de resolución de litigios, basado en predicciones supone que la aplicación del derecho sería la misma, cuando en realidad las circunstancias de cada caso concreto son diferentes.

4.2.2 Contratación y despidos a través de IA

Es una realidad el uso de IA para el análisis de la productividad de los trabajadores y llevar a cabo despidos para aumentar el rendimiento de las empresas. A través del medio de

[72]MIRÓ F.: "*Inteligencia Artificial y Justicia Penal: Más allá de los resultados lesivos causados por robots*" en Revista de Derecho Penal y Criminología, núm. 20, 2018, pp. 87 y ss.

comunicación "*The Verge*" se dieron a conocer numerosos casos de despidos en EEUU por parte de la empresa Amazon. En estos despidos se señalaba la "falta de productividad" como argumento del despido. En un almacén de Estados Unidos la empresa llevó a cabo un procedimiento de recopilación y tratamiento de datos para determinar la productividad de sus empleados siendo despedidos los menos productivos. Se emplea esta técnica de *Big Data* para tomar decisiones tan importantes como un despido sin pasar por la supervisión y confirmación de un supervisor. El sistema parece muy eficaz a la hora de evaluar la productividad, pero es evidente que no es capaz de analizar las situaciones particulares de los trabajadores. Por ello parece precipitado que un despido se funde en estos motivos, pudiendo dar lugar a discriminaciones.

Pese al riesgo que supone emplear IA en la gestión de personal[73], en la actualidad, se ha extendido el uso de IA en los recursos humanos de las empresas[74]. Con la inclusión de estas técnicas se pretende dejar atrás la parcialidad y los prejuicios ante determinadas personas y situaciones. Con el uso de algoritmos se crea una falsa idea de neutralidad ya que la decisión, al no ser humana, parece que no puede discriminar a las personas. Pero la realidad es que los algoritmos responden a la creación a base de criterios humanos por lo que pueden llevar a discriminaciones que vulneren los derechos de los individuos[75].

De lo anteriormente expuesto cabe concluir que el uso de IA en el ámbito de contratación y despido debe de estar bajo el control y supervisión humano, puesto que, pese a la certeza de estas decisiones, puede que se hayan dejado atrás determinados aspectos puntuales contrarios al principio de igualdad. No parece coherente que se realice un despido en función de productividad comparando personas que son diferentes y que desarrollan trabajos también diferentes. En la misma línea, respecto a la contratación, la legislación no puede permitir el uso de algoritmos en el proceso de selección que lleven a la discriminación de ciertas personas. A modo de ejemplo, cabe mencionar el uso de algoritmos que descartaban a ciertas mujeres casadas o con pareja en un proceso selectivo debido a la mayor probabilidad de quedar embarazadas ya que eso resultaría perjudicial para la producción de la empresa. Este criterio podría suponer una discriminación de las mujeres casadas o con

[73]ARIAS, B. ROSETE, A. MARTINEZ, R.: "*Propuesta Informática para seleccionar personal por competencias utilizando técnicas de Inteligencia Artificial*" en Revista Ingeniería Industrial, núm. 2, 2006, pp. 34 y ss.
[74]AGREDA, S.: "*Nuevos retos en el reclutamiento y selección de personal: perspectivas organizacionales y divergencias éticas*" disponible en: https://pdfs.semanticscholar.org/7e3f/c2dba3a11b27dd8f377b1e7ef68e9c00cfd7.pdf
[75]COTINO, L.: "Riesgos e impactos del Big Data, La Inteligencia Artificial y la Robótica. Enfoques, Modelos y Principios de la respuesta del Derecho" en Revista General de Derecho Administrativo, núm. 50, 2018, pp. 1 y ss.

pareja, que el algoritmo considera más propensas a tener hijos, respecto de los hombres y las mujeres no casadas o sin parejas.

4.3 Derecho al olvido

Comenzaremos este apartado a partir de la definición de Derecho al olvido[76], entendido como un derecho que tiene un sujeto que ha consentido el tratamiento de sus datos, a que el responsable de ese tratamiento modifique o elimine ciertos datos que le incumben. Se produce por tanto un cambio en el consentimiento que permitía el tratamiento de datos que se estaba realizando puesto que el interesado considera que el uso de esos datos ya no es necesario o no es acorde al fin por el que se captaron y esta situación puede estar produciendo alguna vulneración de los derechos de quien cedió los datos.

En este sentido se pronuncia el Tribunal de Justicia de la UE en la sentencia relativa al caso Google[77] diciendo que "*el interesado tiene derecho a que la información en cuestión relativa a su persona ya no esté, en la situación actual, vinculada a su nombre por una lista de resultados, obtenida tras una búsqueda efectuada a partir de su nombre, sin que la apreciación de la existencia de tal derecho presuponga que la inclusión de la información en cuestión en la lista de resultados cause un perjuicio al interesado"*. Esto es posible en virtud de los derechos recogidos en los artículos 7 y 8 de la Carta de Derechos Fundamentales de la UE por los que se establece la protección de la vida familiar y los datos personales. Concretamente, el articulo 8 apartado 2, hace referencia al acceso y rectificación de los datos tratados.

El Derecho al olvido[78] nace por tanto como una garantía necesaria dentro de la realidad en la que se procesan cantidad de datos debido en gran parte a los avances tecnológicos. Algunas de las cuestiones que se han planteado alrededor de este derecho al olvido parten de los datos tratados y difundidos por los motores de búsqueda, por ejemplo, a través del caso Google. Muchos de los usuarios de esta herramienta habían cedido cierta información personal que queda accesible asociada a sus datos identificativos, por ello, pedían que esa información se retirará o se modificará. Algunas de estas peticiones se

[76]MATUE, L.C.: "¿Qué es realmente el Derecho al Olvido?" en Revista de Derecho Civil, num. 2, 2016, pp. 189
[77]STJUE 13 de mayo de 2014, asunto C-131/12 Google Spain, S.L. y Agencia Española de Protección de datos.
[78]GUASCH, V. SOLER, J.R.: "El Derecho al olvido en Internet" en Revista de Derecho Uned, num. 16, 2015, pp. 990 y ss.

fundamentaban en proteger la seguridad de las personas puesto que existían ciertos datos relativos a sanciones administrativas, sanciones disciplinarias de funcionarios de prisiones, datos relativos a casos de violencia de género, etc. que se encuentran asociados a la identidad de las personas.

Por tanto, el derecho al olvido se estructura como necesario puesto que sirve como herramienta para evitar o reducir las posibles vulneraciones de otros derechos. Es evidente que tras haber otorgado el consentimiento para el procesamiento de datos pueden darse situaciones en las que otros derechos se vean comprometidos. El uso de determinados datos puede afectar a la intimidad personal y familiar, al honor, a la propia imagen, etc. y ante estas posibles vulneraciones el derecho al olvido permite eliminar o modificar esa información de modo que no se produzca una injerencia.

Respecto a la legislación nacional encontramos la Ley Orgánica de Protección de Datos que, si bien no reconoce el concepto de "derecho al olvido", sí que reconoce los derechos a la oposición y cancelación que guardan relación con el mismo. En el artículo 5 de la LOPD se señala la posibilidad de "*ejercitar los derechos de acceso, rectificación, cancelación y oposición*". Así mismo, en virtud artículo 6 de la LOPD, se recogen los supuestos en que el interesado puede pedir la cancelación de los datos. Estos derechos entran dentro de los tradicionales denominados "ARCO" derecho de acceso, rectificación, cancelación y oposición.

En este mismo sentido se establece el Reglamento General de Protección de Datos[79] que tiene como finalidad por un lado la protección de datos de los ciudadanos y, por otra parte, garantizar la prosperidad del mercado digital de la Unión Europea evitando el falseamiento de la competencia. En lo que respecta al derecho al olvido dentro del RGPD se posibilita tanto el derecho a la cancelación y oposición de datos como la eliminación de estos datos cuando supongan una injerencia en los derechos fundamentales. Se trata por tanto de una garantía que trata de proteger la privacidad de los ciudadanos.

La regulación tendente a poder decidir sobre los datos que incumben a los interesados resulta necesaria puesto que parece coherente que los datos relativos a una persona no son estáticos y pueden cambiar y, por ello, el interesado debe tener derecho a rectificar esa información para proteger de esta forma sus derechos. El hecho de que una persona cometa un error y este quede plasmado en Internet para siempre es algo que marcaría a la persona

[79]SANCHO, M.: *Garantías legales del concepto de Privacidad: entre el Derecho al Olvido y el nuevo Reglamento Europeo de Protección de Datos*" en Actualidad Jurídica Iberoamericana, núm. 9, 2018, pp. 176 y ss.

de por vida. Un ejemplo bastante claro sería la persona que ha sufrido una sanción y que tras cumplir el correspondiente castigo esa sanción siga apareciendo asociada a su nombre a través de la información que encontramos en la red. No parece que esto sea lo correcto puesto que el sujeto ha cumplido con su responsabilidad y ha dejado atrás esos hechos. De igual forma, una persona que ha consentido el tratamiento de cierta información puede ver, con el transcurso del tiempo, como esa información afecta a otros derechos como puede ser el honor o la intimidad familiar que este quiere proteger, y, por tanto, el ordenamiento jurídico debe brindarle la posibilidad de ajustar esa información a la nueva situación.

5.- ANÁLISIS DE JURISPRUDENCIA E INFORMES DE LA UE EN RELACIÓN CON EL BIG DATA

5.1 Apropiación y uso de Big Data: Caso IMS Health S.L.

En el presente apartado presentaré dos casos relativos a la empresa norteamericana *IMS Health* en lo que respecta a la protección de datos a través de la propiedad intelectual y el efecto que tiene sobre el mercado.

La empresa americana *IMS Health*, actualmente IQVIA[80], centra su trabajo en el uso de la tecnología dentro del ámbito sanitario. Su actividad se concreta en el uso de *Big Data* para optimizar la conexión entre los centros médicos y los pacientes.

La Audiencia Provincial de Madrid, el 8 de junio de 2015, dictó sentencia condenatoria[81] por la que condenaba a la empresa tecnológica *IMS Health* al pago de 5 millones de euros a la empresa *INFONIS SL* por apropiación indebida de una base de datos y la posterior comercialización de los datos contenidos en la misma. La indemnización responde al 65% de los beneficios generados con la comercialización de los productos a través de esos datos y, además, se retiraron en primera instancia los productos que tuvieran como base la información empleada indebidamente. Esta apropiación indebida es fruto de una relación comercial iniciada en 2004 en la que *IMS Health* tuvo acceso a una base de datos denominada ZBSales, propiedad de *INFONIS*, en la cual se almacenaba información relativa a la distribución de medicamentos y demás información sanitaria de numerosos centros médicos españoles. Ambas empresas finalizaron su relación empresarial en el año 2007 pero la empresa *IMS Health* continuó empleando la información contenida en dicha base de datos para la elaboración de productos y su comercialización. Tras conocerse estos hechos la empresa perjudicada, *INFONIS*, presentó una demanda contra *IMS Health* en base a la vulneración de la ley de propiedad intelectual, así como actos por competencia desleal.

La empresa INFONIS alegaba un derecho "*sui géneris de propiedad intelectual*" que se apoyaba en los artículos 10 y 12 del Real Decreto Legislativo 1/1996 correspondiente al texto refundido de la Ley de Propiedad Intelectual. Esta protección se basa en el esfuerzo realizado por la empresa en la recopilación y ordenación de los datos en la base de datos, por ese

[80]Información sobre la empresa IQVIA disponible en: https://www.iqvia.com/es-es/about-us
[81]Sentencia n.º 682/2010 Juzgado de lo Mercantil nº2, Audiencia Provincial Madrid, 2015

esfuerzo se brinda la posibilidad de proteger tal información pudiendo prohibir el uso de los datos que contenga, así como traspasar o ceder temporalmente los mismos.

La empresa *IMS Health* recurrió en casación ante el Tribunal Supremo[82] que inadmitió el recurso confirmando la Sentencia de la Audiencia Provincial, así como los argumentos esgrimidos en la Sentencia condenatoria. Presenta gran importancia debido a que sienta las bases para la consideración y valoración del derecho "*sui géneris de propiedad intelectual*" al determinar conceptos relativos a las características que ha de presentar la base de datos para que esta sea protegida por la ley. En la Sentencia se señala en el Fundamento Jurídico segundo la vulneración del derecho "*sui generis*" al haber copiado la información de la base de datos para la elaboración del producto. Se señala así mismo que la base de datos goza de esa protección "*sui generis*" debido a que la empresa *INFONIS* había llevado a cabo una inversión importante para la creación de la misma. Así mismo, la empresa *IMS Health* copió los datos de tal forma que se correspondían con total exactitud con los contenidos en la base de datos lo que facilitó la prueba. Esta Sentencia establece las pautas para la protección de un instrumento tan necesario como son las bases de datos en el ámbito del *Big Data*. La necesidad de acumular los datos estructurados para facilitar su procesamiento supone un gran esfuerzo e inversión por las empresas que debe ser protegido para evitar su apropiación indebida. Por tanto, lo que indica la Sentencia es que no se protegen los datos en sí, puesto que la titularidad de los datos no se establece con su recopilación y almacenamiento, más bien, se viene a proteger la "inversión sustancial" a través del derecho "sui generis" previsto en el artículo 133 de la Ley de protección de datos. Las bases de datos son creaciones empresariales que deben ser protegidas evitando la copia de datos de una base de datos a otra puesto que esta acción supondría un aprovechamiento de la inversión ajena.

Por tanto, considero importante recalcar que esta Sentencia supone el establecimiento de unos criterios de protección a través del derecho "sui generis" que afectan de forma amplia al *Big Data* y, además, establecen garantías dentro de la economía de Big Data puesto que brinda protección a quien realiza una inversión en esta tecnología. Esta protección se basa en el derecho específicamente reconocido en relación con las bases de datos. Con este derecho se garantiza la protección del esfuerzo o inversión llevada a cabo por el creador de la base de datos, otorgando a este la potestad de ceder este esfuerzo o prohibir su utilización. La especialidad de este derecho es que no se protege el contenido de la base de datos, el contenido de la misma puede ser empleado por otros sujetos sin que se

[82]N.º de Recurso: 2455/2015, 31/01/2018 Sala de lo Civil, Tribunal Supremo

vean afectados los derechos del creador de la base de datos. Es decir, mientras que se protege la propiedad intelectual ordinaria por el esfuerzo llevado a cabo por el autor y por la singularidad de su obra, en este "derecho sui generis" simplemente se protege el esfuerzo realizado en la creación de una base de datos, pudiendo crearse por otros medios una base de datos con la misma información que no afectaría a este derecho por tener su origen en un procedimiento independiente, sin basarse en una base de datos protegida.

Más allá de la Sentencia condenatoria, en cuanto al análisis del caso, creo conveniente analizar el caso desde la perspectiva de la información recopilada ya que afecta a distintos centros médicos y a los pacientes que acuden a los mismos. El uso de esta información por parte de la empresa *IMS Health* para la creación y comercialización de productos supone emplear datos obtenidos para un fin no previsto a la hora de otorgar el consentimiento. La comercialización de datos, de esta forma, puede suponer una injerencia por parte de la empresa *IMS Health* que puede llegar a afectar a la privacidad de los pacientes de los centros médicos incluidos en la base de datos. El hecho de trabajar con datos almacenados acorde a las normativas de tratamiento de datos no otorga *per se* un derecho al tratamiento para fines distintos de los concretados en el momento de captación de los mismos. Considero que la normativa de protección de datos tiene que centrar la protección de los datos en el momento de la captación, pero también en el momento de su almacenamiento ya, sea mediante el cifrado de la base de datos, como con la prohibición de apropiarse de los datos sin consentimiento aun teniendo acceso a ellos, como en el mencionado caso.

Otro de los casos relativos a la empresa norteamericana *IMS Health* es el asunto C-418/1[83] que planteaba una cuestión prejudicial relativa al artículo 102 TFUE (anterior artículo 82 del Tratado Constitutivo de la Comunidad Europea), el cual dispone que: "*será incompatible con el mercado común y quedará prohibida, en la medida en que pueda afectar al comercio entre los Estados miembros, la explotación abusiva, por parte de una o más empresas, de una posición dominante en el mercado común o en una parte sustancial del mismo*".

La cuestión surge en este caso en Alemania cuando *IMS Health* elabora una "estructura de segmentos" que supone un método de organización de datos a través de una estructura específica para poder ser empleados de manera eficiente. La empresa norteamericana empleó esa estructura cediéndolas a farmacias y centros médicos y se han

[83]Asunto C-418/01 Sentencia del Tribunal de Justicia (Sala Quinta) de 29 de abril de 2004

convertido en estructuras de "uso corriente" dentro del mercado sanitario alemán. *Pharma Intranet Information*, que fue absorbida por *NDC Health GmbH* & *Co*, comenzó a comercializar estudios de mercado que tenían como base la estructura de segmentos creada por *IMS Health*. En un primer momento, los Tribunales alemanes prohibieron la utilización de esta estructura a la empresa NDC y esta presentó una denuncia ante la Comisión de las Comunidades Europeas, alegando que la negativa de IMS a concederle una licencia de utilización de la estructura infringía el artículo 82 CE. La Comisión a través de la Decisión 2002/165/CE de carácter urgente por la situación en la que se tomó como medida provisional la concesión de una licencia de utilización puesto que al haberse convertido en una estructura de uso generalizado la negativa en la concesión de la licencia afectaría a la competencia en el mercado.

A raíz de las circunstancias expuestas IMS presentó una decisión prejudicial con el objeto de prohibir a NDC la utilización de la estructura creada por la empresa norteamericana. El problema reside en que la empresa IMS ostenta una posición dominante en el mercado y el tribunal ha de analizar si la negativa en otorgar una licencia de uso de la estructura de datos supone una práctica abusiva. La negativa en la concesión de una licencia de uso supondría una barrera de entrada al mercado casi infranqueable puesto que el esfuerzo de adaptación que deberían de hacer los clientes de NDC adaptándose a una nueva estructura de datos sería muy alto.

El Tribunal entra a valorar aspectos relevantes respecto al *Big Data* en lo que se refiere a la utilización de procedimientos a la hora de tratar los datos y la protección de esas técnicas, así como la negativa en ceder dichas creaciones. El Tribunal expone que habrá que valorar si el producto o servicio, la estructura de datos en este caso, es indispensable para llevar a cabo la actividad en el mercado o si por el contrario existe alguna alternativa que sea viable. En este caso concreto IMS elaboró una estructura de datos que supone un instrumento de *Big Data* único ya que de él dependen las compañías farmacéuticas del mercado ya que ayudaron en su creación y extendieron su uso. Por tanto, ante esa situación, estas compañías farmacéuticas tendrán que realizar un esfuerzo desmesurado para obtener una estructura alternativa por parte de NDC que también debería adaptar esa estructura no obteniendo rentabilidad, haciendo inviable la entrada en el mercado. Estos aspectos habrán de ser valorados a la hora de determinar si la conducta llevada a cabo por IMS negando la licencia de uso supone una actuación abusiva.

El Tribunal, respecto a la cuestión relativa al derecho exclusivo sobre la estructura en base al derecho de propiedad intelectual señala que la negativa en la cesión de una licencia por parte de una empresa con posición dominante en el mercado no puede constituir en si mismo un abuso de posición dominante. Pero lo que si que puede suceder es que el ejercicio del derecho exclusivo, en determinadas circunstancias, dé lugar a comportamientos abusivos. Estas circunstancias se concretan en tres requisitos: obstaculización en la entrada en el mercado de un nuevo producto, negativa injustificada a ceder el derecho exclusivo y exclusión de toda competencia en el mercado.

El Tribunal resolvió las cuestiones prejudiciales dejando claros los criterios que han de valorarse a la hora de determinar si la negativa en la cesión de una licencia de uso supone un abuso de posición dominante, en función del artículo 102 TFUE:

- *"La empresa que ha solicitado la licencia pretenda ofrecer, en el mercado del productos o servicios nuevos que el titular del derecho de propiedad intelectual no ofrece y para los cuales existe una demanda potencial por parte de los consumidores;*
- *La negativa no esté justificada por consideraciones objetivas*;
- *La negativa pueda reservar al titular del derecho de propiedad intelectual el mercado de suministro de datos sobre ventas de productos farmacéuticos en el Estado miembro de que se trate, excluyendo toda competencia sobre éste*."

A raíz del análisis de las dos Sentencias se puede considerar que la protección que otorga la propiedad intelectual a los datos procesados mediante Big Data se centra en el esfuerzo que se ha invertido para procesar los mismos, pero, esta protección no tiene por qué extenderse a los sistemas empleados para procesar la información. Es decir, la protección que brinda la propiedad intelectual se centra en evitar la apropiación indebida del esfuerzo ajeno, pero cede cuando un sujeto externo necesita los mecanismos utilizados para el procesamiento y almacenamiento de los datos para proteger con ello la economía de mercado evitando barreras de entrada infranqueables y garantizando la libre competencia en la economía del *Big Data*.

5.2 Informes y Política de la Unión Europea

Es una realidad que los datos se han convertido en un activo de gran potencial dentro de la economía global, es por ello que la Unión Europea[84], conocedora de esta realidad, trata de potenciar y desarrollar la tecnología y herramientas para que el tratamiento de información ayude a la consecución de los objetivos de la Unión. La Comisión de la Unión Europea considera que el valor que tienen los datos se adquiere a través del propio procesamiento de los datos, en cada etapa de tratamiento de datos. Por tanto, la creación y uso de herramientas y tecnología eficiente que pueda tratar estos datos supondrá mejorar los aspectos tradicionales de la economía logrando optimizar y maximizar el rendimiento. El objetivo de potenciar estas tecnologías es la consecución de una transformación y adaptación de la industria de servicios europeos en base a estos datos, así como ampliar la productividad con el uso de técnicas de IA y *Big Data* en el ámbito empresarial. Otro punto que trata de potenciarse es la investigación e innovación que, apoyándose en técnicas de *Big Data* será más rápido y eficiente.

Este proceso de transformación digital depende del establecimiento de un marco normativo que garantice, por un lado, la protección de los ciudadanos y, por otro lado, la aportación de los medios y la seguridad necesaria a las empresas para adentrarse en el uso del *Big Data*. Es evidente que la protección de los derechos establecidos en marco de la Unión han de ser una prioridad, por ello la protección de datos será siempre una prioridad. En segundo lugar, también habrá que tener en cuenta otro de los objetivos de la Unión como es la creación de un espacio económico común en el que facilitar la comercialización de datos. Por ello, la Unión Europea, se centrará en la creación de un mercado único de datos con el que garantizar la competitividad de la Unión. Con esta idea se garantiza la disponibilidad de datos tanto para actividades económicas como sociales y, a su vez, se permite controlar a las empresas que procesan los datos a través de una normativa común.

La Unión Europea ve en los datos un enorme potencial que puede emplearse para la mejora de servicios sanitarios, sistemas de transporte, reducir el coste de servicios públicos, etc. Para la consecución de estos objetivos la Unión trata de crear un marco normativo en el que regular aspectos como el poder de tratamiento de datos, el acceso a los datos y la reutilización de datos. La Unión invierte en la creación de un proyecto[85] relativo a las

[84] "*Shaping Europe's digital future: Big Data*" disponible en: https://ec.europa.eu/digital-single-market/en/big-data

[85] "*Iniciativa Europea de Computación en la Nube: construir en Europa una economía competitiva de los datos y del conocimiento*" disponible en: https://ec.europa.eu/transparency/regdoc/rep/1/2016/ES/1-2016-178-ES-F1-1.PDF

herramientas de procesamiento y almacenamiento de datos para el aprovechamiento efectivo de los datos en el marco de la Unión Europea.

En el año 2004 la Comisión Europea en el intento de adaptar la Unión Europea al avance de las nuevas tecnologías planteó a un grupo de trabajo el análisis de las Tecnologías convergentes[86]. Ese informe aborda la evolución de las tecnologías hacia un objetivo común que es la expansión a los distintos ámbitos sociales para lograr la optimización y adaptar el entorno de la UE al avance de estas tecnologías. El autor de este informe es Alfred Nordmann quien considera necesario la integración en convergencia de las distintas ciencias para trabajar en conjunto y lograr, además de una optimización general, el desarrollo humano en el marco de la Unión. El informe señala la importancia de las Tecnologías Convergentes para el futuro de la sociedad, indicando además que ha de someterse a las políticas comunes de la UE para ayudar a la consecución de las metas. En este informe se señala la importancia de acompañar normativamente los avances logrados por la tecnología que habrá de hacerse, tanto desde los organismos europeos como desde los Estados miembros. Toda esta creación normativa ha de respetar los derechos y principios europeos, así como la idea de unificación normativa de la Unión. Uno de los aspectos en los que se centra el presente informe es en el de señalar la importancia de emplear la tecnología para la optimización de las actividades tradicionales y, no tanto, en la mejora de las capacidades humanas, ya que esto último no supone una prioridad. Parece exponer de esta forma que la tecnología tendrá que ser implementada de tal forma que el beneficio obtenido sea general, para toda la sociedad, y no emplear la tecnología para el desarrollo humano particular tratando de aumentar sus capacidades.

En última instancia, en febrero del año 2020, la UE ha emitido la estrategia europea en relación con los datos[87]. Se trata de fijar la idea sobre un mercado de datos de la UE, así como de adaptar la política de la Unión para afianzar la economía de datos.

---

[86]Informe "*Converging Technologies Shaping the Future of European Societies by Alfred Nordmann, Rapporteur*" disponible en: https://op.europa.eu/en/publication-detail/-/publication/7d942de2-5d57-425d-93df-fd40c682d5b5

[87]"*A European strategy for data*" disponible en: https://ec.europa.eu/info/sites/infofiles/communication-european-strategy-data-19feb2020_en.pdf

5.3 Influencia de Facebook en las elecciones a la presidencia de USA y el Brexit

La empresa "*Cambridge Analytica*"[88] centra su trabajo en el ámbito de las TICs concretamente interesa en relación con el *Big Data* sus actividades relacionadas con el procesamiento de datos para optimizar campañas publicitarias, así como campañas políticas, mayormente en USA. Es relevante para este trabajo conocer la influencia que tuvo esta empresa en la campaña electoral que llevó a la presidencia a Donald Trump, así como en el proceso por el que Reino Unido salió de la Unión Europea. Es importante para este trabajo conocer estos casos puesto que el *Big Data* puede resultar determinante en un proceso legalmente regulado como es el proceso electoral o afectando a la democracia a través de actividades que pueden suponer una injerencia para la privacidad y lo derechos de los ciudadanos.

La empresa "*Cambridge Analytica*" llevó a cabo una recopilación masiva de datos a través de la red social Facebook basando esa captación de datos en fines académicos[89]. Esta situación no es tolerable en el marco normativo europeo de protección de datos puesto que supone captar datos indicando que su uso será para fines distintos de los que finalmente fueron empleados. Esta empresa aprovechó el desconocimiento de los usuarios, así como los escasos medios de control y garantías de esta red social para llevar a cabo una recopilación masiva de información que posteriormente sería aprovechada para ajustar las campañas publicitarias o políticas en relación, tanto como las elecciones presidenciales de USA como en el *Brexit*.

Desde distintos medios estadounidenses como, *The New York Times* y *The Observer*, se señaló aún más allá, indicando que la información obtenida se empleó para llevar a cabo "manipulaciones psicológicas". Lo cierto es que es complicado argumentar que la campaña de Trump triunfara porque se llevaron a cabo manipulaciones psicológicas, pero sí que se puede argumentar que dentro de ese proceso electoral existió una ventaja obtenida por la información captada de manera indebida. Esta información fue obtenida a través de "tests" dentro de la plataforma de Facebook que además de emplearse para obtener cierta información otorgaba permisos para acceder a la información personal de los usuarios, así como a la de los amigos dentro de la plataforma. Esto supuso un alcance notable dentro de

[88] "*Facebook, Cambridge Analytica y tus datos: Todo lo que debes saber del escándalo y cómo te afecta a ti*" disponible en: https://www.cnet.com/es/noticias/facebook-cambridge-analytica-trump-lo-que-debes-saber/
[89] "*El escándalo de Cambridge Analytica*" disponible en: https://www.bbc.com/mundo/noticias-43472797

la población estadounidense, llegando casi a un 20% de la población. La información recopilada alcanzaba desde simples publicaciones hasta mensajes privados de los usuarios. Esta información, según la política de Facebook, no podía ser empleada fuera del ámbito de la red social, pero al no existir ningún control por parte de la empresa se comercializó con esos datos.

La información obtenida indebidamente fue empleada para ciertos fines que plantean dudas sobre la legalidad de estos usos. La información recopilada se empleó para crear publicidad personalizada para los distintos usuarios y, además, se crearon y difundieron noticias falsas que afectaron a los competidores políticos de Donald Trump. Esta cuestión guarda relación con el *Big Data* puesto que puede verse una conexión entre el uso de esta tecnología y las "*fakes news*" que en la actualidad han aparecido por la gran cantidad de medios de difusión existentes gracias a las tecnologías y las pocas medidas de seguridad relativas al contenido de la información. En este sentido parece que la Unión Europea quiere marcar ciertas directrices para controlar el uso de estas noticias falsas dentro de la Unión. La Comisión creó un Grupo de expertos[90] en el año 2017 que tiene como finalidad el análisis de la propagación de noticias falsas y que parece que va encaminado a identificar el grado de perjuicio que pueden causar y, en tal caso, adoptar una normativa que regule ciertos aspectos de esta divulgación de información falsa siempre respetando la libertad de expresión e información.

Para concluir con este apartado quiero resaltar la relación existente entre el *Big Data* y estos acontecimientos. El *Big Data* fue empleado para captar y recopilar todos los datos obtenidos a través de la red social Facebook que fueron utilizados posteriormente para influenciar en los asuntos mencionados. Tras esa captación se elaboraron perfiles y predicciones de votos en las que el *Big Data* también fue el responsable del procesamiento. Una vez obtenida información sobre la tendencia de votos se llevaron a cabo ajustes en la campaña electoral de Donal Trump y en la campaña en favor de aceptar el Brexit. Esta optimización de las campañas fue acompañada de un proceso de desacreditación a través de la divulgación de información falsa.

Considero conveniente señalar que hay varios derecho y aspectos legales que pueden verse comprometidos por los hechos mencionados. En primer lugar, la obtención de la información de ese modo supone una captación indebida puesto que se aleja de los fines de

[90] "*Grupo de expertos para el control de las fakes new*" disponible en https://ec.europa.eu/digital-single-market/en/news/call-applications-selection-members-high-level-group-fake-news

la red social en que se obtuvieron y no se indica en ningún momento el propósito de la captación de información. Además, se emplea el *Big Data* para alcanzar datos de las personas que cayeron en la trampa y alcanzar a la información de sus amigos dentro de la plataforma. Esto supone un grave riesgo para la privacidad y la intimidad de las personas puesto que se accede a datos personales y se trata de obtener su intención de voto e ideas políticas sin pedir autorización. En segundo lugar, tras tener esta información valiosa se gestiona a través del *Big Data* el procesamiento de esos datos para obtener la información requerida y con ella adoptar una campaña acorde al propósito que se quiere lograr. Esta idea no parece ir en contra de ninguna normativa puesto que estamos, simplemente, ante una forma de ajustar una campaña para que sea más efectiva, pero al provenir la información de una fuente ilícita esta campaña no debería de ser posible. Además, el hecho de emplear técnicas de divulgación de información falsa tomando como base la información recopilada es una técnica agresiva que en ciertas ocasiones no sería aceptable puesto que llega a afectar a los intereses y derechos de terceras personas, influyendo en su opinión y decisiones por medio de información falsa, por ello podría ser interesante regular estos aspectos en el futuro para evitar su uso. La difusión de información falsa puede afectar a los derechos al honor, propia imagen e intimidad. La divulgación de información indebida puede suponer por tanto la vulneración de ciertos derechos y por ello la persona afectada tiene derecho a que se modifique o rectifique la información divulgada.

5.4 Sentencia del Tribunal de Justicia (Gran Sala) de 13 de mayo de 2014

Se plantea el caso con relación al asunto C-131/12[91] por el cual se platea al Tribunal de Justicia una cuestión prejudicial acerca de la interpretación de ciertos preceptos de la normativa europea a raíz de un procedimiento judicial en España entre un ciudadano español y Google por mantener en su buscador información relativa a esta persona, información que en el momento de platear el litigio carecía de veracidad puesto que se trataba de un asunto de 1998 que ya fue resuelto. La información que aparecía en los resultados de búsqueda era relativa a ciertos créditos pendientes por parte de un ciudadano español en favor de la

[91]AZURMENDI, A.: "*Por un «derecho al olvido» para los europeos: Aportaciones jurisprudenciales de la Sentencia del Tribunal de Justicia europeo del caso Google Spain y su recepción por la Sentencia de la Audiencia Nacional española de 29 de diciembre de 2014*" en Revista de Derecho Político, núm. 92, 2015, pp. 275 y ss.

Seguridad Social. Esta persona pagó su deuda, pero la información que aparecía en la red no fue retirada y esto afectaba a su reputación.

A raíz de estos hechos la AEPD estimó la reclamación del ciudadano e indicó que Google debía de adoptar las medidas necesarias para que este tipo de información no apareciese en los resultados de búsquedas. Google realiza un procesamiento de datos y obtiene y ordena estos resultados de acuerdo a los intereses de la compañía y con esta reclamación la AEPD lo que pedía era que Google adaptase estos criterios de búsqueda. Google recurrió la resolución ante la Audiencia Nacional y se planteó ante el Tribunal de Justicia una cuestión prejudicial.

En la Sentencia del Tribunal[92] se indica que el motor de búsqueda de Google lleva a cabo un "tratamiento de información" en el sentido descrito en el artículo 2, letras b) y d), de la Directiva 95/46/CE[93]. Es responsable por tanto de ese tratamiento de información y, el Tribunal, no acepta el argumento esgrimido por la empresa Google sobre que el tratamiento se aleje de las actividades propias de la empresa establecida en la Unión Europea (según la interpretación del artículo 4, apartado 1, letra a), de la Directiva 95/46). El Tribunal plantea la figura del derecho al olvido dentro del marco de actuación de la empresa Google ya que no trata directamente con los datos personales de los individuos, pero sí que brinda la posibilidad de acceder a los mismos. Por ello, el Tribunal viene a marcar la idea de que las personas tendrán derecho a pedir al motor de búsqueda Google que se retire de los resultados de búsqueda la información relativa a su persona. Con esto se trata de proteger la vida privada de los individuos evitando que los usuarios obtengan información personal de otras personas a través de los buscadores.

Google considera que esta limitación afecta a sus intereses económicos de una forma importante puesto que sus criterios de búsquedas y resultados se encuentran asociados a un procesamiento de datos muy amplio en el que dan prioridad a las empresas que invierten a través de publicidad u otros medios en la empresa Google. Por ello el Tribunal señala que habrá que realizar una ponderación entre los intereses de los individuos y los intereses de los motores de búsqueda para poder valorar que interés resulta afectado y valorar sobre la

[92]Sentencia del Tribunal de Justicia (Gran Sala) de 13 de mayo de 2014 en relación al asunto C-131/12 https://www.abogacia.es/wp-content/uploads/2014/05/Sentencia-131-12-TJUE-derecho-al-olvido.pdf

[93]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 disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:31995L0046&from=EN

necesidad de eliminar la información. Por ello habrá que analizar cada caso en concreto con el objetivo de identificar el tipo de información que pretende ser eliminada de los motores de búsqueda y si esa información verdaderamente afecta a la vida privada de las personas o a sus derechos al honor, intimidad o a la protección de datos personales; entonces, habrá de proceder a eliminar esos resultados de búsqueda.

Parece que con esta Sentencia el Tribunal de Justicia viene a establecer[94] que el derecho a la protección de datos se impone al derecho a la información en los casos en los que efectivamente estemos ante determinados datos que estén dentro del marco de protección de ese derecho.

El Tribunal indica que en el sentido que marca la Directiva 95/46 el gestor de un motor de búsqueda, en este caso Google, está obligado a "modificar o eliminar de la lista de resultados obtenida tras una búsqueda efectuada a partir del nombre de una persona vínculos a páginas web, publicadas por terceros y que contienen información relativa a esta persona, también en el supuesto de que este nombre o esta información no se borren previa o simultáneamente de estas páginas web, y, en su caso, aunque la publicación en dichas páginas sea en sí misma lícita". Para llevar a cabo esa modificación de la información tendrá que valorarse el derecho del individuo que pide que esa información se elimine teniendo que suponer un perjuicio para el interesado que esa información esté dentro de los resultados de búsqueda. Dándose estos requisitos este derecho prevalecerá sobre el interés económico del motor de búsqueda y el derecho a la información.

[94]CORDOBA CATROVERDE, D.: "*Los Retos de la Protección de Datos en Internet. Caso Google Spain y Derecho al Olvido*" disponible en Anuario de la Facultad de Derecho de la Universidad Autónoma de Madrid, núm. 21, 2017, pp. 223 y ss.

6.- CONCLUSIONES

Para concluir con este trabajo quiero mostrar las opiniones y valoraciones que he alcanzado a lo largo del análisis jurídico que he realizado sobre el concepto del *Big Data* y su influencia en los distintos ámbitos.

En un primer lugar, he logrado entender que el *Big Data* pese a ser un concepto tecnológico, puesto que indudablemente tiene su base en la tecnológica, ha logrado extenderse a todos los ámbitos económicos, sociales, políticos, etc. Considero que es inevitable que la tecnología acabe complementando a los medios y procedimientos tradicionales puesto que la tecnología es sinónimo de eficacia y productividad y, teniendo en cuenta esta expansión, de igual forma el *Big Data* se extenderá a muchos sectores para lograr actividades más eficientes gracias al procesamiento de información. Todo esto me lleva a otra conclusión y es que el *Big Data* no es un fenómeno emergente que vaya a implantarse en el futuro, sino que más bien es un fenómeno que ya se ha instaurado dentro de nuestra sociedad y, por tanto, las medidas normativas adoptadas responden a las necesidades que se han planteado a raíz de observar los problemas y lagunas suscitadas por el uso del *Big Data*. Pese a estos avances normativos, siguen existiendo lagunas e indeterminaciones que han de ser analizadas desde todas las perspectivas, realizando una ponderación entre los intereses relativos a los derechos de las personas, los nuevos mercados, las nuevas políticas, etc. Esta consideración tiene su base en como se han adaptados los mercados y los medios de comunicación a la tecnología y el *Big Data*. En general, dentro de las empresas con mayor capitalización bursátil sobresalen empresas tecnológicas como Apple, Microsoft, Amazon, etc. que destacan por haber desarrollado la tecnología del *Big Data* en los últimos años. Estas empresas conocedoras del gran valor de los datos han ofrecido servicios para tener acceso a datos de las personas y con ello poder, tanto optimizar su actividad, como comercializar con esa información. Muchas empresas han entrado en el "mercado de los datos" ofreciendo servicios de captación y procesamiento de datos para otras empresas con el fin de obtener ventajas competitivas y maximizar beneficios. Esto ha supuesto que el Derecho de la competencia también se vea afectado debido a la aparición de nuevas técnicas basadas en el *Big Data* que pueden afectar al mercado, como puede ser la fijación de precios a través de algoritmos o el reparto de mercado en base a los datos obtenidos.

En segundo lugar, al estudiar el tema del *Big Data* se puede llegar a la dudosa consideración de que únicamente se ve afectado el derecho fundamental relativo a la

protección de datos puesto que el *Big Data* se basa principalmente en datos, en la información relativa a las personas. Una vez analizado el concepto, conociendo en qué consiste el *Big Data*, se pueden identificar injerencias en otros derechos fundamentales. La protección de estos datos debe ser eficaz pues pueden vulnerarse derechos como la intimidad tanto personal como familiar a través de la captación y procesamiento de datos. El problema es que, como ya he mencionado, el Big Data se emplea en multitud de procedimientos y actividades por lo que pueden verse comprometidos otros derechos o garantías como, por ejemplo, los principios constitucionales de igualdad y no discriminación establecidos en el artículo 14 CE que pueden verse afectados en determinados procesos selectivos en los que se emplea un procedimiento basado en *Big Data*, mediante el uso de algoritmos, para la selección de personal.

Por otra parte, otra de las conclusiones alcanzadas es que el *Big Data* puede emplearse para llevar a cabo conductas y actividades de forma más productiva respetando la legalidad, pero también, puede emplearse para ejecutar conductas ilícitas que afecten a las libertades y derechos de las personas. Por ejemplo, sería acertado el uso por parte de las instituciones estatales de la tecnología de *Big Data* para recopilar información sobre la ciudadanía y con ello distribuir el gasto potenciando los servicios más necesarios y liberando parte de este gasto de servicios que en determinadas zonas o a determinados núcleos de población no les resultan necesarios. Por el contrario, aprovechar la tecnología de *Big Data* para llevar a cabo conductas de fijación de precios supone una conducta ilícita y difícil de identificar puesto que la fijación de precios no surge de un pacto expreso entre empresas, sino que surge del análisis de los datos del mercado por parte de diferentes empresas, así como del establecimiento de algoritmos que regulen el precio dando como resultado una conducta contraria a la prohibición de fijación de precios.

Con estos ejemplos pretendo introducir la idea de que el *Big Data* es una herramienta útil pero peligrosa que debe de emplearse dentro de unos límites que necesariamente tienen que estar marcados por una normativa de ámbito supraestatal. La tecnología elimina las fronteras estatales, la conexión a través de Internet permite tener acceso desde cualquier parte del mundo a información de cualquier Estado. Esta realidad supone que los datos fluyen por la red sin poder controlar la forma en que son captados y procesados. Es por ello que hay que valorar los esfuerzos de la Unión Europea por crear un marco normativo que permita el flujo de datos garantizando los derechos fundamentales de las personas. En este sentido considero interesante la idea marcada por la Unión de brindar una protección a todos los sujetos afectado más allá de su nacionalidad. Pese a los avances, considero que el trabajo

normativo tiene que seguir desarrollándose y, además, considero necesario un órgano que controle los flujos de datos para poder aplicar la normativa correctamente. Hay que tener en cuenta que uno de los mayores riesgos que plantea el *Big Data* es que, en muchas ocasiones, las fuentes de los datos son personas que actúan sin tener una conciencia de su actuación y, por tanto, pueden verse vulnerados determinados derechos sin que las personas afectadas evidencien tal injerencia. Considero que existe una triple necesidad: extender y desarrollar la normativa relativa a protección y transferencia de datos, establecer un órgano a nivel europeo o internacional que controle la transmisión de estos datos y, por último, la difícil tarea de concienciación hacia las personas sobre los riesgos en la cesión de datos.

En este sentido considero igualmente que las empresas tienen dos responsabilidades principalmente, primero, respetar la normativa en relación con la captación de los datos y, segundo, proteger los datos captados de tal forma que solo puedan emplearse para los fines específicos por el sujeto a quien se le otorgó la cesión de los datos. La normativa en este sentido tiene que abarcar de una forma más especifica el hecho de que las empresas tienen que garantizar que no se comercializa con la información sin el consentimiento de quien cedió la información. Para ello será necesario incidir en la creación de órganos que controlen los flujos de datos y eviten sucesos como los mostrados en este trabajo de apropiación indebida de información en las redes sociales.

Otro de los ámbitos que se ve afectado en gran medida es el político, a lo largo del trabajo se han analizados las posibles influencias positivas del *Big Data* dentro de la democracia, optimizando los servicios públicos y logrando cubrir las necesidades de los ciudadanos que al final es el objetivo de una democracia. El *Big Data* puede emplearse como instrumento que potencie la participación ciudadana en numerosos asuntos políticos, puesto que puede emplearse para tomar decisiones acorde a los intereses populares pero, a su vez, el tomar como base el *Big Data* para justificar la toma de decisiones puede ser algo peligroso puesto que la información recopilada no tiene por qué responder a la opinión general, es más, probablemente esté profundamente marcada por los intereses de quien captó la información y quien estableció los algoritmos que recopilan, analizan y procesan esa información. Con todo esto quiero señalar que, pese a que la tecnología y el *Big Data* pueden emplearse en un futuro como mecanismos de una posible democracia directa, debe de establecerse un gran control sobre estos mecanismos para evitar cualquier tipo de influencia y vulneración de los derechos. Es por ello por lo que en este trabajo se han analizado conductas como las de la administración Trump, así como la de determinados grupos en relación con el Brexit que han llevado a cabo políticas de concienciación y propaganda

empleando los macro datos como un instrumento para dañar a la oposición. Considero que el *Big Data* es por tanto una herramienta poderosa, muy difícil de controlar, y que por ello puede resultar interesante que se establezcan tanto órganos de control de flujo de datos como tribunales que conozcan específicamente asuntos en los que la cuestión del litigio verse sobre datos y su procesamiento a través de la tecnología, es decir, tribunales que conozcan asuntos específicamente sobre *Big Data*.

Por otra parte, considero que otros órganos judiciales deben ser cautelosos a la hora de aplicar el *Big Data* dentro de sus actividades. Esta referencia nace de la consideración de que puede ser correcto emplear el *Big Data* para agilizar los procedimientos judiciales, pero, a su vez, considero que no puede permitirse una generalización y establecimiento de criterios en la resolución de casos. Cada litigio tiene unas circunstancias específicas que no podemos obviar y que habrán de ser analizadas concretamente sin asociar unas circunstancias a un resultado de otro litigo puesto que se perdería la neutralidad e independencia de los órganos judiciales sometiendo los resultados de los diferentes litigios a resultados previos que presentan características comunes.

En tercer lugar, considero conveniente analizar una de las cuestiones más importantes acerca del Big Data y que no es otra que el valor de los datos. Los datos tienen un valor que en muchos casos no es conocido. Es evidente que los datos aisladamente no presentan un alto valor, pero es el procesamiento que se da a esos datos a través del Big Data el que proporciona un alto valor a los mismos. En ocasiones se basa la captación de datos en ofrecer servicios "gratuitos" a cambio de obtener acceso a los datos del usuario. Con este intercambio parece que el servicio obtenido supera con creces al "precio" pagado, pero considero que esto no es así puesto que habrá que analizar el coste real que supone a la empresa ofrecer ese servicio y el beneficio total obtenido con la recopilación de los datos en el momento en que el usuario emplea el servicio y cuando no está empleándolo. La conclusión que he alcanzado es que basar la captación de datos en el hecho de ofrecer un servicio gratuito es una técnica peligrosa que encierra un coste oculto y que, por ello, debe de ser controlada para evitar abusos. Al igual que ofrecer servicios gratuitos para obtener información, emplear clausulas generales poco precisas e indeterminadas considero que es una práctica en auge, como ya hemos visto en el trabajo concretamente en las redes sociales los usuarios aceptan un tratamiento generalizado de datos sin conocer de forma específica el uso que se dará a esa información. Considero que la normativa tiene que incidir en el consentimiento específico y, además, tendrá que establecer un "deber de control" por parte

de las empresas con el que garantizar el cumplimiento de la normativa y el control de uso de esos datos para los fines establecidos.

En cuarto lugar, en lo que se refiere al uso de IA, así como de técnicas de "machine learning" esto supone ceder a la tecnología la toma de ciertas decisiones, así como elaborar predicciones. El hecho de que se procese la información y se tomen decisiones puede suponer en según que campos un gran riesgo que habrá de ser analizado y desarrollado por las normativas para evitar que la tecnología tome decisiones sin fundamento que terminen afectando a los derechos de las personas. Emplear esta tecnología en determinados procedimientos puede afectar a los principios de igualdad, mérito o transparencia ya que las decisiones obtenidas no se ajustan a un criterio objetivo por provenir de un medio tecnológico sin "conciencia" y sin "opiniones". Como ya he mencionado en este trabajo, la tecnología supone dejar atrás los medios tradicionales y eliminar ciertas actividades que se desarrollaban por personas, pero esta idea no significa que la tecnología no se encuentre influida por los humanos. El *Big Data* es producto de la creación humana y, como tal, la influencia de los creadores de herramientas y algoritmos fijan valores y opiniones en estos. Con esto quiero dejar clara la idea de que la tecnología no es sinónimo de objetividad y, por tanto, la normativa y los órganos de control deberán controlar con firmeza las decisiones que provengan de la IA para garantizar que no existe discrecionalidad oculta bajo la falsa idea de "objetividad tecnológica".

Este trabajo no se centra simplemente en el análisis de los riesgos del *Big Data,* sino que he querido enfocar las distintas cuestiones de una forma objetiva para conocer los riesgos y las ventajas del *Big Data* y con ello poder conocer los aspectos en que el derecho tiene que desarrollarse para no quedar anticuado. Entiendo el *Big Data* como sinónimo de cambio dentro del derecho puesto que de una manera positiva puede afectar a los derechos tradicionalmente reconocidos como en el caso de la pandemia del Covid-19. El hecho de emplear esta tecnología para luchar contra la pandemia supone una restricción en lo que se refiere a derechos y libertades, pero, debido a la gravedad de la situación, puede ser jurídicamente aceptable plantear tales limitaciones si con ello se salvaguardan efectivamente otros derechos. Creo que junto a la nueva normalidad los organismos gubernamentales habrán de desarrollar aplicaciones basadas en la información para gestionar de una manera más eficiente el servicio sanitario y con ello impedir una saturación del sistema como la acontecida. Para conseguir que estas aplicaciones sean precisas y viables es necesario acompañar el desarrollo tecnológico con un desarrollo normativo que realice una ponderación sobre los derechos afectados teniendo en cuenta que la protección de datos, así

como el derecho a la intimidad puede verse afectado en este caso para salvaguardar la actividad sanitaria y con ello garantizar una protección efectiva del derecho a la vida.

A raíz de lo expuesto considero que existen sectores en los que el *Big Data* podrá avanzar de forma rápida y funcional como hemos visto en relación con el "mercado de datos" que se basa en la comercialización de información y por ello la Unión Europea ha tratado de adaptar la normativa comunitaria a esta realidad, posibilitándolo este mercado gracias a la novación normativa. Pero, por otra parte, el *Big Data* aplicado al ámbito sanitario entraña riesgos por el valor y la sensibilidad de los datos manejados, así como las restricciones de derechos que pueden darse en el caso de controlar nuestra situación permanentemente, así como el contacto con otras personas.

Con todo esto quiero terminar señalando que el Big Data plantea un análisis especifico, valorando en que ámbitos puede emplearse y en que ámbitos no puede tener cabida. La respuesta a esta cuestión no es absoluta, sino que más bien habrá que acudir al derecho vigente para valorar si el uso del Big Data en un ámbito especifico presenta las garantías y controles necesarios que respeten los derechos y valores establecidos.

BIBILIOGRAFIA

OBRAS GENERALES

BARNETT H.: "Constitutional and Administrative Law", ed. Taylor & Francis, Londres, 2019

BRENNAN T. DIETERICH W.: "Correctional Offender Management Profiles for Alternative Sanctions (COMPAS)" en SINGH/KRONER/WORMITH (Cords): "Recidivism Risk/Needs Assessment Tools" ed. Wiley-Blackwell, Nueva Jersey, 2018

FERNÁNDEZ E.: "Big Data: Eje estratégico en la industria audiovisual" ed. UOC, Barcelona, 2017

GIL, E.: "Big data, privacidad y protección de datos" ed.: AEPD y AEBOE, Madrid, 2016

JOYANES, L.: "Big Data, Análisis de grandes volúmenes de datos en organizaciones", ed. Alfaomega, México, 2013

LÓPEZ A., GUTIÉRREZ I.: "Elementos de Derecho público", ed. Marcial Pons, Madrid, 2002

MARÍN H.: "Discrecionalidad administrativa", ed. Universidad Externado de Colombia, Bogotá, 2007

MEGÍAS, J.: "Construcción de redes sociales garantes de la privacidad" en LOMBARTE/MARTÍNEZ (Cords): "Derecho y redes sociales", Thomson Reuters, Navarra, 2010

O´NEIL, C.: "Armas de destrucción matemática" ed. Crown Books, EE.UU.,2016

QUADRA-SALCEDO, T/PIÑAR, J L. (Dirs): "Sociedad Digital y Derecho" ed. Red.es y BOE, Madrid, 2018

SARTONI, G.: "¿Qué es la Democracia?", ed. Penguin Random House, Ciudad de México, 2012

ARTÍCULOS

AGREDA, S.: "Nuevos retos en el reclutamiento y selección de personal: perspectivas organizacionales y divergencias éticas"

ARIAS, B. ROSETE, A. MARTINEZ, R.: "Propuesta Informática para seleccionar personal por competencias utilizando técnicas de Inteligencia Artificial" en Revista Ingeniería Industrial, núm. 2, 2006

AZURMENDI, A.: "Por un «derecho al olvido» para los europeos: Aportaciones jurisprudenciales de la Sentencia del Tribunal de Justicia europeo del caso Google Spain y su recepción por la Sentencia de la Audiencia Nacional española de 29 de diciembre de 2014" en Revista de Derecho Político, núm. 92, 2015

CLAICI, A.: "Big Data y Política de la Competencia" en Papeles de Economía Española, nº 157, 2018

COLMENAREJO, R.: "Ética aplicada a la gestión de datos masivos" en Anales de la Cátedra Francisco Suárez, nº 52, 2018

CORDOBA CATROVERDE, D.: "Los Retos de la Protección de Datos en Internet. Caso Google Spain y Derecho al Olvido" disponible en Anuario de la Facultad de Derecho de la Universidad Autónoma de Madrid, núm. 21, 2017

COTINO, L.: "Riesgos e impactos del Big Data, La Inteligencia Artificial y la Robótica. Enfoques, Modelos y Principios de la respuesta del Derecho" en Revista General de Derecho Administrativo, núm. 50, 2018

DURÁN, F.J.: "Big Data aplicado a la mejora de los servicios públicos y protección de datos personales" en Revista de la Escuela Jacobea de Posgrado, núm. 12, 2017

GARCIA F.: "Big Data y democracia" en Revista internacional de Filosofía núm. 23, 2019

GUASCH, V. SOLER, J.R.: "El Derecho al olvido en Internet" en Revista de Derecho Uned, num. 16, 2015

HILDEBRANDT, M.: "Esclavos de los macrodatos. ¿O no?" en Revista de Internet, Derecho y política, nº 17, 2013

JIN X,WAH BH, CHENG X,WANG Y.: "Significance and Challenges of Big Data Research" en "Big Data Research" núm. 2, 2015

KÖRBER, T.: "Data, Platforms and Competition Law"

MARTINEZ, L./SANCHO, M.: "El nuevo concepto de onerosidad en el mercado digital. ¿Realmente es gratis la App?" en InDret nº 1, 2018

MARTINEZ, MC.: "Algoritmos, Big Data y el derecho de la competencia"

MATUE, L.C.: "¿Qué es realmente el Derecho al Olvido?" en Revista de Derecho Civil, num. 2, 2016

MERINO GOMEZ, G.: "Nuevos desafíos en torno al Big Data" en Revista de Derecho y Genoma Humano, núm. extraordinario, 2019

MIRÓ F.: "Inteligencia Artificial y Justicia Penal: Más allá de los resultados lesivos causados por robots" en Revista de Derecho Penal y Criminología, núm. 20, 2018

MORTE FERRER, R.: "¿Protección de datos/privacidad en la época del Big Data, IoT, wearables…? Sí, más que nunca" en Revista Dilemata, num. 24, 2017

NIÑO, M. e ILLARRAMENDI, A.: "Entendiendo el big data"

ORBE, A.: "Ética y Big Data",

PEREZ, F.: "Ciberseguridad: Ransomware"

PICCOTI, L.: "Los derechos fundamentales en el uso y abuso de las redes sociales en Italia: aspectos penales" en Revista de Internet, Derecho y Política, nº16, 2013

RICHARDSON, R. Y NORTH, M.: "Ransomware: Evolution, Mitigation and Prevention"

SANCHO, M.: Garantías legales del concepto de Privacidad: entre el Derecho al Olvido y el nuevo Reglamento Europeo de Protección de Datos" en Actualidad Jurídica Iberoamericana, núm. 9, 2018

"Shaping Europe's digital future: Big Data"

SOLIS, V: "Técnicas de inteligencia artificial para optimizar la eficiencia del procedimiento de selección para la contratación de obras públicas" en Revista Interfases, núm. 11, 2018

JURISPRUDENCIA

Asunto C-418/01 Sentencia del Tribunal de Justicia (Sala Quinta) de 29 de abril de 2004

Recurso: 2455/2015, 31/01/2018 Sala de lo Civil, Tribunal Supremo

Sentencia 292/2000, de 30 de noviembre

Sentencia n.º 297/2016 de 7 de diciembre de 2016, Juzgado de lo Mercantil, Barcelona

Sentencia n.º 682/2010 Juzgado de lo Mercantil nº2, Audiencia Provincial Madrid, 2015

STJUE 13 de mayo de 2014, asunto C-131/12 Google Spain, S.L. y Agencia Española de Protección de datos

881 N.W.2d 749 (2016) WI 68 STATE of Wisconsin, Plaintiff-Respondent, v. Eric L. LOOMIS, Defendant-Appellant

LEGISLACIÓN

Carta de los Derechos Fundamentales de la Unión Europea de 26 de octubre 2012

Carta Europea "European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their environment", Estrasburgo, 3-4 diciembre 2018

Constitución Española

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Estrasburgo, 28 de enero de 1981

Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal

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

Ley 7/1998, de 13 de abril, sobre condiciones generales de la contratación

Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias

Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016

Resolución del Parlamento Europeo, de 12 de febrero de 2019, sobre una política industrial global europea en materia de inteligencia artificial y robótica (2018/2088)

Tratado Constitutivo de la Comunidad Europea de 12 de junio de 1985

Tratado de Funcionamiento de la Unión Europea del 26/10/2012

Tratado de la Unión Europea, versión consolidada del 30.3.2010

Otra información

"A European strategy for data"

Agencia Europea para los Derechos Fundamentales: "Big Data: Discrimination in data-supported decisión making", Austria, 30 de mayo de 2018

"Grupo de expertos para el control de las fakes new"

Informe "Converging Technologies Shaping the Future of European Societies by Alfred Nordmann, Rapporteur" disponible

"Iniciativa Europea de Computación en la Nube: construir en Europa una economía competitiva de los datos y del conocimiento"