FACULTAD DE DERECHO

¿SUPONE EL BIG DATA UN NUEVO DESAFÍO PARA EL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS PERSONALES?

Autor: Victoria Blanc Braquehais

4º E1-BL

Filosofía del Derecho

Tutora: Vanesa Morente Parra

Madrid

Junio 2019

INDICE

LISTADO DE ABREVIATURAS

AEPD: Agencia Española de Protección de Datos

CE: Constitución Española

EM: Estado Miembro

OCDE: Organización para la Cooperación y el Desarrollo Económicos

RPD: Reglamento General de Protección de Datos

TC: Tribunal Constitucional

TFUE: Tratado de Funcionamiento de la Unión Europea

TJUE: Tribunal de Justicia de la Unión Europea

UE: Unión Europea

1. INTRODUCCIÓN

La rápida evolución tecnológica y la globalización han planteado nuevos retos para la protección de datos personales. La magnitud de la recogida y del intercambio de datos personales ha aumentado de manera significativa. La tecnología permite que tanto las empresas privadas como las autoridades públicas utilicen datos personales en una escala sin precedentes a la hora de realizar sus actividades. Las personas físicas cada vez difunden un volumen cada vez mayor de información personal a escala mundial. La tecnología ha transformado tanto la economía como la vida social, y ha de facilitar aún más la libre circulación de datos personales dentro de la Unión y la transferencia a terceros países y organizaciones internacionales, garantizando al mismo tiempo un elevado nivel de protección de los datos personales.[1]

El frenético avance de las tecnologías de la información en las últimas décadas ha irrumpido en todas las esferas de nuestra vida cotidiana y profesional, cambiando nuestra perspectiva.

Concretamente, el surgimiento del *big data* (término acuñado para referirse a la manipulación de una cantidad masiva de datos) ha supuesto uno de los cambios más importantes y revolucionarios en el panorama internacional, ha resultado ser un verdadero fenómeno. Este tratamiento masivo de datos nos ha llevado a tener que afrontar una serie de peligros referidos a la protección de nuestra privacidad, es decir, el contenido de nuestros datos personales.

"La violación de la privacidad puede ser imprevisible, puede producirse a largo término y no sólo se origina en una esfera individual, sino que también afecta a una esfera colectiva y afecta al conjunto de la sociedad."[2]

En este trabajo vamos a exponer cómo han revolucionado las nuevas tecnologías nuestros derechos fundamentales a la intimidad y a la protección de datos personales. Para ello, estudiaremos la gran relevancia de estos derechos fundamentales, su normativa a nivel nacional e internacional; los problemas que ha supuesto el *big data* y qué medidas se han tomado al respecto para solucionarlo.

[1] Considerando sexto del Reglamento (UE) 2016/279, de 27 de abril de 2016, de Protección de Datos Personales

[2] Suárez-Gonzalo, S., "Big Social Data: límites del modelo *notice and choice* para la protección de la privacidad" El profesional de la información, v.26, n.2, 2017 pp. 283-292, p.285

2. DERECHOS FUNDAMENTALES

2.1. El Derecho a la Intimidad

2.1.1 En el ámbito internacional o comunitario

El primer texto que regula el derecho a la intimidad personal y familiar es la **Declaración Universal de Derechos Humanos de 1948, en su artículo 12**[3]: *"Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques."*

Como señala Martínez de Pisón, "en los últimos tiempos, debido al avance tecnológico, la protección del derecho a la intimidad ha adquirido una mayor relevancia social y, consecuentemente, jurídica, que, incluso, supere a otras libertades individuales tradicionalmente mucho más importantes."[4] Este derecho es considerado como uno de los derechos y libertades perteneciente a la primera generación, aquella que se consolida con el Estado Liberal de Derecho.

Definitivamente "la incidencia de las tecnologías de la información en la vida privada de las personas y los problemas derivados de la protección de datos personales ha adquirido una magnitud inimaginable en los últimos años"[5]
La prensa ha ido adquiriendo cada vez mayor interés en entrometerse en el ámbito personal y familiar de las personas; situación que ha acarreado, en especial para las personas que tenían incidencia en la vida pública, numerosos problemas. Por ello se ha desarrollado una preocupación paulatina por la protección de la esfera privada.

Habría que delimitar qué entendemos por derecho a la intimidad. En un primer momento, se centraba en que la prensa no se adentrase dentro de la vida íntima de ciertas personas de carácter público. Se trataba de "proteger un espacio íntimo de la intromisión o

[3] Martínez de Pisón, J., "El derecho a la intimidad: de la configuración inicial a los últimos desarrollos en la jurisprudencia constitucional" *Universidad de la Rioja*, n.32, 2016, pp. 409-430, p. 410
[4] "El derecho a la intimidad: de la configuración inicial a los últimos desarrollos en la jurisprudencia constitucional" cit. 411
[5] "El derecho a la intimidad: de la configuración inicial a los últimos desarrollos en la jurisprudencia constitucional" cit. 412

injerencia de terceros"[6]. Cabe señalar que esta idea no la engloba únicamente el término intimidad, sino que también se utilizan otros como privacidad, vida privada o ámbito íntimo. Con el paso del tiempo, han ido precisándose y especializándose estos términos, para terminar de decantarnos por el de intimidad y el de privacidad[7].

La delimitación del concepto de intimidad no ha estado exenta de discusiones y controversias dando lugar a debates de todo tipo. Pérez Luño hace una adecuada composición de lo que entendemos como intimidad, diferenciando tres esferas diferentes dentro de la misma[8]:

-En primer lugar, tenemos la esfera íntima. "Se constituye como el círculo más cercano a la persona, hace referencia a lo más secreto de la persona, a lo relacionado con sus opiniones, decisiones y acciones más íntimas"[9].

-En segundo lugar, está la esfera privada. Ésta se constituye como "un círculo más amplio en el que el individuo sigue ejerciendo su privacidad, su vida privada, su intimidad personal y familiar y que, por ello, quiere que esté asegurada y protegida frente a terceros"[10].

-En tercer y último lugar, nos encontramos con la esfera individual, supone "el último de los círculos de la intimidad antes de la vida pública, que estaría constituido por otros aspectos vinculados a la misma, como el honor y la imagen personal, que también reflejan la personalidad del individuo"[11].

Fuera del ámbito de estas tres esferas, encontramos la vida pública, en este ámbito no se puede exigir la imposición de límites a la participación de terceros.

De lo deducido en esta clasificación, no siempre nos será fácil poder distinguir el ámbito de una esfera u otra, ya que en algunas ocasiones puede dar lugar a confusión.

[6] "El derecho a la intimidad: de la configuración inicial a los últimos desarrollos en la jurisprudencia constitucional" cit. 412
[7] "El derecho a la intimidad: de la configuración inicial a los últimos desarrollos en la jurisprudencia constitucional" cit. 412
[8] Pérez Luño, A. E., "*Derechos Humanos, Estado de Derecho y Constitución*", TECNOS, Madrid, 1986, p.375
[9] "El derecho a la intimidad: de la configuración inicial a los últimos desarrollos en la jurisprudencia constitucional" cit. 412
[10] "El derecho a la intimidad: de la configuración inicial a los últimos desarrollos en la jurisprudencia constitucional" cit. 412
[11] "El derecho a la intimidad: de la configuración inicial a los últimos desarrollos en la jurisprudencia constitucional" cit. 412

2.1.2 En el sistema constitucional español

A)El artículo 18 CE y sus peculiaridades

El derecho a la intimidad personal y familiar está regulado en el artículo 18 de la Constitución Española (CE) de 1978, siguiendo así el planteamiento establecido en la Declaración Universal de Derechos Humanos de 1948 al recoger este nuevo derecho. Se han planteado a una serie de dificultades para este conjunto de normas, por ello destaca el papel del Tribunal Constitucional.

La estructura del derecho a la intimidad en nuestro sistema constitucional está formada por:

El art.18 CE:

1. *"Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.*
2. *El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito.*
3. *Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.*
4. ***La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.**"*

El citado precepto constitucional tiene una serie de peculiaridades, ya que, como señala Martínez de Pisón "el art. 18 CE garantiza el derecho a la intimidad personal y familiar pero no define ni perfila el significado de la noción de intimidad ni su relación con el resto de manifestaciones de este derecho tan personalísimo"[12]

Asimismo, no está clara la naturaleza singular o plural de los derechos contenidos en el artículo 18 CE: éstos son el derecho al honor, a la intimidad personal y familiar y a la propia imagen. Surgen dudas acerca de si estamos ante un solo derecho individual, el derecho a la intimidad, y que dicho derecho tiene diversas manifestaciones; o si, por el contrario, nos encontramos ante dos o, incluso, tres derechos diferentes.[13] Esta

[12] "El derecho a la intimidad: de la configuración inicial a los últimos desarrollos en la jurisprudencia constitucional" cit. 415

[13] "El derecho a la intimidad: de la configuración inicial a los últimos desarrollos en la jurisprudencia constitucional" cit. 416

controvertida duda no ha estado exenta de polémicas doctrinales, aunque Martínez de Pisón concluye que parece aceptarse la tesis de que el artículo 18 CE regula tres derechos:

-El derecho al honor.

-El derecho a la intimidad personal y familiar.

-El derecho a la propia imagen.

Estos tres derechos constituyen los derechos de la personalidad, el autor afirma que "está superada la teoría de que hay un solo derecho de la personalidad con manifestaciones múltiples".[14] Afirmando, en consecuencia, la pluralidad de derechos en el citado precepto constitucional.

Conviene señalar la especial ubicación del precepto, ya que se encuentra en el Título II, Sección 1ª: "*De los derechos fundamentales y de las libertades públicas*". Ello implica que estos derechos constituyan un bloque de especial protección dado su carácter de fundamentales, siendo ésta la categoría de mayor relevancia de nuestro sistema constitucional. De ahí que la jurisdicción vele por su cumplimiento y persiga su vulneración de una manera especial respecto a otro tipo de derechos.

B)Evolución del derecho a la intimidad en la jurisprudencia constitucional

B.1. Comienzos de la doctrina del Tribunal Constitucional

Ante la ambigüedad sobre el contenido del citado precepto (art. 18 CE), la labor del Tribunal Constitucional tiene un papel decisivo y esencial para la definición y concreción del derecho fundamental.

En general, ya ha hecho una gran labor para la definición de los derechos fundamentales y en la elaboración de un sistema de derechos y libertades públicas de los ciudadanos, fijando el contenido esencial previsto en el artículo 56 CE.

La base de la doctrina construida desde el principio por el Tribunal Constitucional se sustentaba en unos fundamentos básicos [15]:

[14] "El derecho a la intimidad: de la configuración inicial a los últimos desarrollos en la jurisprudencia constitucional" cit.417

[15] "El derecho a la intimidad: de la configuración inicial a los últimos desarrollos en la jurisprudencia constitucional" cit. 418

- Los derechos del art.18 CE son derechos personalísimos o derechos de la personalidad.
- Estos derechos contenidos en el citado precepto están vinculados a la dignidad humana, por lo que está conectado al art. 10 CE y con el conjunto de tratados internacionales sobre derechos y libertades fundamentales.
- Estos derechos implican un espacio propio y reservado.
- Uno de los objetivos de estos derechos es proteger ese ámbito mínimo de las injerencias de terceros, de intromisiones extrañas
- El derecho a la intimidad en el ordenamiento jurídico español no es un derecho de carácter absoluto, sino que su contenido debe responder a estimaciones y criterios arraigados en la cultura de la comunidad.
- Por ello, es esencial la realización de una ponderación que valore los hechos relevantes y equilibre los bienes jurídicos que están en conflicto.

Estos fundamentos se reflejan en la jurisprudencia constitucional, podemos poner como ejemplo varios fragmentos:

Los derechos a la intimidad personal y familiar y a la propia imagen, garantizados por el art. 18.1 de la Constitución, forman parte de los bienes de la personalidad que pertenecen al ámbito de la vida privada. Salvaguardan estos derechos un espacio de intimidad personal y familiar que queda sustraído a intromisiones extrañas[16]

Los derechos a la imagen y a la intimidad personal y familiar quedan reconocidos en el artículo 18 de la Constitución aparecen como derechos fundamentales estrictamente vinculados a la propia personalidad, derivados sin duda de la dignidad de la persona, que reconoce el art. 10 CE, y que implican la existencia de un ámbito propio y reservado frente a la acción y conocimiento de los demás, necesario -según las pautas de nuestra cultura- para mantener una calidad mínima de la vida humana. Se muestran así estos derechos como personalísimos y ligados a la misma existencia del individuo.[17]

[16] FJ 4 de la Sentencia del Tribunal Constitucional 170/1987, de 30 de octubre
[17] FJ 2 de la Sentencia del Tribunal Constitucional 231/1988, de 2 de diciembre

El Tribunal Constitucional insiste en el carácter personalísimo de los derechos del art. 18 CE. Se vinculan a la esfera de la personalidad individual[18]. El TC creó, desarrolló y aplicó este planteamiento del contenido esencial del derecho a la intimidad a un amplio y variado conjunto de supuestos.

B.2. Jurisprudencia Constitucional en los últimos años

En los últimos veinte años, la jurisprudencia constitucional "ha consolidado la línea doctrinal sobre el derecho fundamental a la intimidad personal y familiar". Ha ido concretando y matizando las ideas generales de la doctrina, pudiendo afirmar que ha supuesto una mejoría en la construcción jurídica del derecho, ya que para algunos el planteamiento inicial doctrinal anteriormente explicado no resolvía los problemas planteados en torno a este derecho fundamental por las lagunas del legislador[19].
Martínez de Pisón aclara los cambios más destacados en la jurisprudencia constitucional y que reflejan la creciente preocupación de las amenazas que el *big data* supone al derecho a la intimidad:

- Hay un creciente interés de los ciudadanos por proteger su intimidad, por ello, han aumentado los recursos de amparo con el objeto de proteger los derechos del art. 18 CE.
- La explicación de este aumento sustancial de demandas al respecto es la difícil conexión entre los derechos contenidos en el art. 18 CE (intimidad, honor y propia imagen) y los derechos el art. 20 CE (libertad de expresión y derecho a la información).
- Asimismo, con el avance de las nuevas tecnologías, surge la creciente preocupación por la protección de datos personales que se encuentran en ficheros informáticos y que han dado lugar a la libertad informática[20].
- Por otro lado, cada vez se da más uso al *mecanismo de ponderación de bienes* para resolver los casos que atañen al derecho a la intimidad y a la propia imagen, especialmente, cuando colisionan con otros derechos y libertades.

[18] FJ 3 de la Sentencia del Tribunal Constitucional 21/1992, de 14 de febrero: "la intimidad personal y familiar es, en suma, un bien que tiene la condición de derecho fundamental (art. 18.1 CE) y sin el cual no es realizable, ni concebible siquiera, la existencia en dignidad que todos quiere asegurar la norma fundamental (art. 10.1 CE)".
[19] "El derecho a la intimidad: de la configuración inicial a los últimos desarrollos en la jurisprudencia constitucional" cit. 423
[20] Artículo 18.4 de la Constitución Española

Por último, la referencia constitucional relativa a la intimidad se completa con lo previsto en el art. 20.4 CE: "*4. Estas libertades tienen su límite en el respeto a los derechos reconocidos en este Título, en los preceptos de las leyes que lo desarrollen y, especialmente, en el derecho al honor, a la intimidad, a la propia imagen y a la protección de la juventud y de la infancia."*

Definitivamente, el concepto de privacidad está cambiando debido a la revolución tecnológica, por ello debe establecerse ese límite al derecho de libertad de información, ya que de lo contrario colisionarían ambas libertades.

2.2.Derecho de protección de datos personales

2.2.1. En el ámbito internacional o comunitario

En el ámbito de la Unión Europea, encontramos diversas referencias al derecho de protección de datos, estableciendo ya su carácter fundamental.

"Desde una perspectiva europea, el derecho a la protección de datos personales es un derecho fundamental consagrado en el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea"[21], que indica lo siguiente:

"Artículo 8

Protección de datos de carácter personal:

1. *Toda persona tiene* ***derecho a la protección de los datos de carácter personal*** *que la conciernan.*
2. *Estos datos se* ***tratarán de modo leal, para fines concretos*** *y sobre la base del* ***consentimiento*** *de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación.*
3. *El respeto de estas normas quedará sujeto al* ***control de una autoridad independiente***."

[21] Recio Gayo, M., "*Big Data:* Hacia la protección de datos personales basada en una transparencia y responsabilidad aumentadas", *Revista de Derecho, Comunicaciones y Nuevas Tecnologías*, n.17, 2017, p.9

En el ámbito europeo, este derecho también esta recogido en el artículo 16 del Tratado de Funcionamiento de la Unión Europea (TFUE):

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

Las normas que se adopten en virtud del presente artículo se entenderán sin perjuicio de las normas específicas previstas en el artículo 39 del Tratado de la Unión Europea."

De ambos preceptos podemos sacar varias conclusiones acerca de los aspectos básicos de este derecho. La protección de este derecho como fundamental tiene su base en unos principios para el "tratamiento lícito y legítimo de los datos personales, unas obligaciones exigibles a quien se encarga de su tratamiento, igualmente unos derechos para los titulares de los datos personales". Es necesaria la existencia de una autoridad de control y supervisión independiente que vele por el cumplimiento de la normativa por parte de quienes traten los datos personales, independientemente de su pertenencia al sector público o privado[22]. También cabe destacar la relevancia que ya se le da al consentimiento en la Carta de Derechos Fundamentales de la Unión Europea[23]

Puede concebirse como un derecho autónomo de la privacidad, en el sentido de la Unión Europea, implicando así el control de los datos personales. Recio Gayo resalta que la atención específica debe ponerse en el uso que pueda darse a los datos personales.

[22] "*Big Data:* Hacia la protección de datos personales basada en una transparencia y responsabilidad aumentadas", cit. 10

[23] Su artículo 8.2 ya la menciona como fundamental para que haya un tratamiento de datos personales adecuado.

"La protección de la privacidad de los datos personales en el mundo occidental tiene una característica común: comparten el paradigma de autogestión de la privacidad que se basa en el modelo *notice and choice*."[24]

La normativa europea en materia de protección de datos personales ha alcanzado una gran relevancia y trascendencia a nivel internacional, un claro reflejo de ello es la jurisprudencia reciente del Tribunal de Justicia de la Unión Europea (TJUE)[25], como muestran sus sentencias en los asuntos *Google Spain*[26]*, Weltimmo*[27]*, Schrems*[28] *o Verein für Konsumenteninformation*[29].

2.2.2. En el sistema español

Elena Gil afirma que este derecho a la protección de datos ha sido definido por nuestros tribunales, estableciendo que "consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de estos datos proporcionar a un tercero, sea el Estado o un particular, o un particular, o cuáles puede este tercero recabar, permitiendo también al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o su uso. Su carácter de derecho fundamental le otorga determinadas características, como la de ser irrenunciable y el hecho de prevalecer sobre otros derechos no fundamentales"[30].

A nivel nacional, cabe destacar la figura de la Agencia Española de Protección de Datos (AEPD). Es un organismo público, creado en 1983, cuyas funciones y competencias tienen como objetivo el efectivo cumplimiento de la Ley Orgánica de Protección de Datos de Carácter Personal en España. Se trata de un ente público independiente que actúa con independencia de la Administración Pública en el ejercicio de sus funciones. Su ámbito

[24] "Big Social Data: límites del modelo notice and choice para la protección de la privacidad" cit.285
[25] De Miguel Asensio, P. A., "Competencia y derecho aplicable en el Reglamento General de Protección de Datos de la Unión Europea" *Revista Española de Derecho Internacional*, vol. 69/1, 2017, Madrid, pp.75-108, p.75
[26]Sentencia del Tribunal de Justicia de la Unión Europea C-131/12 de 13 de mayo de 2014, *Google Spain* (Diario Oficial de la Unión Europea, 7 de julio de 2014)
[27] Sentencia del Tribunal de Justicia de la Unión Europea C-230/14, de 1 de octubre de 2015, *Weltimmo* (Diario Oficial de la Unión Europea, 16 de noviembre de 2015)
[28] Sentencia del Tribunal de Justicia de la Unión Europea C-362/14, de 6 de octubre de 2015, *Schrems*, (Diario Oficial de la Unión Europea, 6 de octubre de 2015)
[29]Sentencia del Tribunal de Justicia de la Unión Europea C-191/15 de 28 de julio de 2016 (Diario Oficial de la Unión Europea, 26 de septiembre de 2016)
[30] Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre de 2000

de aplicación es de carácter estatal. A su vez, España también cuenta con agencias de protección de datos de carácter autonómico en Cataluña y en el País Vasco.[31]
La AEPD protege los derechos de acceso, rectificación, limitación, oposición, supresión ("derecho al olvido"), portabilidad y oposición al tratamiento de decisiones automatizadas. Asimismo, establece las obligaciones que deben cumplimentar aquellos que tratan datos (organizadores, empresas, administraciones públicas).[32]

Como hemos mencionado, su principal objetivo es velar por el cumplimiento de la normativa de protección de datos por parte de los responsables de los denominados ficheros, algunos de estos responsables son las entidades públicas, las empresas privadas o las asociaciones.
Además, también controlan la aplicación de la normativa a fin de garantizar el derecho fundamental a la protección de datos personales de los ciudadanos.

La AEPD lleva a cabo sus potestades de investigación fundamentalmente a petición de los ciudadanos, aunque también está facultada para actuar de oficio. La Agencia, al ser un ente jurídico independiente, se relaciona con el Gobierno a través del Ministerio de Justicia.

[31] Agencia Española de Protección de Datos https://www.aepd.es/agencia/index.html
[32] Agencia Española de Protección de Datos (https://www.aepd.es/reglamento/cumplimiento/index.html)

3. BIG SOCIAL DATA

3.1.Concepciones generales, qué se entiende por Big Data

El impacto de las nuevas tecnologías ha supuesto un cambio revolucionario presente en todos los aspectos de nuestra vida cotidiana tanto personal como profesional. Se han creado nuevas herramientas que tienen como principal característica la inmediatez. Lo que en tiempos anteriores suponía grandes inversiones de esfuerzo y tiempo actualmente pueden resolverse en cuestión de segundos.
Este continuo e imparable avance se ve reflejado en todas las esferas de nuestra realidad, incluida la esfera jurídica.

Podemos afirmar que el *Big data* puede englobar ese gran cambio e impacto tecnológico, es un concepto que hace referencia al manejo de grandes cantidades de información, Elena Gil lo define como "el conjunto de tecnologías que permiten tratar cantidades masivas de datos provenientes de fuentes dispares, con el objetivo de poder otorgarles una utilidad que proporcione valor".[33]
Es importante resaltar que este concepto alude al uso de una cantidad masiva de datos, que con los métodos tradicionales de almacenamiento de información sería imposible de manejar. Concretamente, el término *big data* puede traducirse como datos masivos, es un "término que se refiere al enorme aumento en el acceso y uso automatizado de la información. Se refiere a las gigantescas cantidades de datos digitales controladas por las empresas, autoridades y otras organizaciones que están sujetos a análisis extensivos" (International Working Group on Data Protection in Telecommunications, Documento de trabajo sobre datos masivos y privacidad).[34]

Se crean nuevas herramientas que pueden asumir y explotar tal cantidad masiva de datos. En el contexto del *big data*, una de esas herramientas es el uso de algoritmos, nos permiten llegar a conocer más información. Una de las grandes novedades que nos aporta la utilización de los algoritmos es lo que se conoce como *machine learning*, ello puede

[33] Gil González, E., *Big data, privacidad y protección de datos*, BOLETIN OFICIAL DEL ESTADO, Madrid, 2016 (p.15)
[34] "*Big Data:* Hacia la protección de datos personales basada en una transparencia y responsabilidad aumentadas" cit. 12

definirse como aprendizaje computacional. La citada herramienta "nos permite identificar y predecir tendencias y correlaciones que pueden crear un perfil de la persona a la que se refieren los datos personales o predecir su comportamiento"[35].
"Dichas herramientas han sido aprovechadas por las grandes empresas, como Google o Facebook, que han podido descubrir nuevas formas de valorizar los datos."[36]Pero no sólo se potencia el *Big data* en el sector privado, las Administraciones Públicas también han sabido sacar beneficio de los avances tecnológicos mejorando así la eficiencia en cuestiones como la protección ciudadana o la asistencia sanitaria.

Elena Gil menciona tres elementos del *big data* que esclarecen sus rasgos fundamentales: "variedad, volumen y velocidad":[37]
En primer lugar, la **variedad** alude a que los datos que son analizados son de distinta naturaleza, se combinan tanto datos estructurados[38] como no estructurados[39].
En segundo lugar, el **volumen** se refiere en la masividad, la gran cantidad de datos que se analizan y utilizan gracias a los nuevos instrumentos de análisis proporcionados por las tecnologías de la información.
Por último, la **velocidad** supone la rapidez con la que pueden crearse y analizarse esta gran cantidad de datos de naturaleza diversa. Antes, había que invertir mucho más tiempo. Antes del desarrollo de las tecnologías de la información era imposible que estas tres variables pudiesen combinarse de manera simultánea, esta dificultad ha sido solventada con el *big data*.

En definitiva, el *big data* "sigue siendo visto como una revolución, implica cambios en muchos sentidos y da lugar a un debate internacional para poder establecer un marco adecuado para la innovación, la privacidad y la protección de datos personales."[40]
Estamos pasando a una realidad en la que prevalecen los tratamientos de datos masivos, dichos tratamientos están en plena expansión y crecimiento ascendente. Recio Gayo

[35] "*Big Data*: Hacia la protección de datos personales basada en una transparencia y responsabilidad aumentadas". cit.12
[36] "*Big data, privacidad y protección de datos"*, cit. 29
[37] Gil González, E., *Big data, privacidad y protección de datos,* cit.p.20
[38] Los datos estructurados son aquellos que pueden ser ordenados y estructurados fácilmente, todo está identificado y es de fácil acceso
[39] Los datos no estructurados son aquellos que no tienen una estructura interna identificable
[40] "*Big Data*: Hacia la protección de datos personales basada en una transparencia y responsabilidad aumentadas"., cit. 4

afirma que "Nos encontramos ante datos personales masivos y tratamientos analíticos, propiciados por la imparable y constante evolución de las tecnologías de la información". En el informe de la EOPCAST se señala que los datos masivos lo son en dos sentidos diferentes. "Por un lado, son masivos en cuanto a la cantidad y variedad de datos disponibles para su tratamiento. Y, por otro lado son masivos en cuanto a la extensión del análisis que puede ser aplicado a dichos datos, en última instancia para hacer las deducciones y sacar conclusiones".

A continuación, vamos a exponer los beneficios y peligros e inconvenientes que ha supuesto la revolución del Big social data

3.2. Beneficios:

Es evidente que el *big data* nos proporciona numerosos avances y nuevas oportunidades que se traducen en un beneficio tangible. "La capacidad para almacenar y analizar grandes cantidades de datos puede ser benéfica para la sociedad"[41]. Entre ellos podemos destacar los siguientes:

Por un lado, nos ofrece una eficacia e inmediatez que desemboca en una mayor precisión en los rendimientos de todo tipo de recursos, nos proporciona tanto a las personas físicas como a las empresas una mayor agilidad para la consecución de determinadas actividades. El análisis de los datos masivos permite desvelar lo que aquellos pueden decir. Según la Conferencia de Autoridades de Protección de Datos y Privacidad "el Big Data implica una nueva forma de ver la información, revelando aquella que antes era difícil de extraer o que estaba oculta"[42].

Los datos personales masivos y su tratamiento analítico puede proporcionar importantes beneficios, que se traducen en oportunidades de innovación en el caso de servicios electrónicos, como por ejemplo las aplicaciones de los dispositivos móviles, como nuevas formas de tratar

[41] "*Big Data:* Hacia la protección de datos personales basada en una transparencia y responsabilidad aumentadas", cit.4
[42] "*Big Data:* Hacia la protección de datos personales basada en una transparencia y responsabilidad aumentadas", cit.11

enfermedades, llegando a reducir costes de tratamientos que no han sido accesibles para todas las personas[43].

La eficiencia de sus herramientas de análisis permite estudiar fenómenos a gran escala, vislumbrar atributos y patrones latentes en los datos e inferir información que las personas no han difundido de forma explícita. Por consiguiente, datos que observados de forma aislada parecen inocuos, procesado pueden revelar gran cantidad de información[44].

Gracias al *big data* pueden predecirse la propagación de epidemias, descubrir los graves efectos secundarios de medicamentos y combatir la contaminación en las grandes ciudades[45]. En definitiva, nos permite un amplio abanico de posibilidades que sin estos nuevos sistemas no serían posibles.

3.3.Riesgos o peligros:

A pesar de los numerosos avances y beneficios que ha supuesto el surgimiento del *big data,* no podemos pasar por alto que también debe enfrentarse a determinados peligros o retos:

En consonancia con Miguel Recio Gayo, "El uso indiscriminado del *big data* puede causar discriminación contra las personas o falta de equidad debido a la incorrecta asociación con un grupo determinado"[46]. Tal como ha observado la Conferencia de Autoridades de Protección de Datos y Privacidad en la Resolución sobre *big data* "el *big data* también puede usarse en formas que generan una preocupación importante respecto a la privacidad de las personas y los derechos civiles, y a las protecciones contra la discriminación y las vulneraciones al derecho a trato igual"[47]

[43] "*Big Data*: Hacia la protección de datos personales basada en una transparencia y responsabilidad aumentadas". cit.4
[44] "Big Social Data: límites del modelo *notice and choice* para la protección de la privacidad" cit. 284
[45] "*Big Data*: Hacia la protección de datos personales basada en una transparencia y responsabilidad aumentadas" cit. 4
[46] "*Big Data*: Hacia la protección de datos personales basada en una transparencia y responsabilidad aumentadas". cit. 11
[47] "*Big Data*: Hacia la protección de datos personales basada en una transparencia y responsabilidad aumentadas" cit. 11

Asimismo, como apunta Suárez-Gonzalo, el *big data* "Supone un problema social para la protección de los datos personales y un desafío para la ordenación jurídica en materia de privacidad"[48].

Por otro lado, cuando el tratamiento de datos se usa con fines poco claros o de manera irresponsable, es cuando surge el riesgo de que su uso pueda materializarse en graves consecuencias para la persona. Recio Gayo resalta que "el riesgo está en el uso que se dé a los datos masivos una vez que han sido objeto de un tratamiento analítico"[49].

Como más adelante desarrollaremos, con el surgimiento de las redes sociales se plantean peligros como la suplantación de identidad, la difusión no consentida de fotografías o el ciberacoso. Concretamente, el ciberacoso o ciberbullying suponen, dada la aparente falta de responsabilidad en el entorno de Internet, una manera más fácil para que las personas que cometen este tipo de ilícitos puedan eximirse de la responsabilidad, ya que es muy sencillo ocultar su identidad en las redes sociales bajo un nombre o apodo falso. Por ello, deben reforzarse las medidas de seguridad en el entorno tecnológico o ciberseguridad.

Las características de la realidad virtual nos ha llevado a la denominación "sociedad de riesgo" y un aumento de la preocupación tanto de legisladores y juristas en lo referido a la protección, entre otros, del derecho de protección de datos personales, como de los propios usuarios, que empiezan a tomar conciencia de los posibles perjuicios que puede suponer la circulación de datos sin ningún tipo de control ni garantías[50].

3.4.Las redes sociales como reflejo de la revolución Big Data

3.4.1. Consideraciones generales

Uno de los principales aspectos a destacar del *big data* es que ha cambiado nuestra manera de comunicarnos entre nosotros, tanto a nivel personal en nuestra intimidad como a nivel profesional en las empresas y en nuestros propios trabajos. Efectivamente, uno de los grandes cambios de la presente década es la aparición de las redes sociales. Durán Arroyo

[48] "Big Social Data: límites del modelo *notice and choice* para la protección de la privacidad" cit. 284
[49] "*Big Data*: Hacia la protección de datos personales basada en una transparencia y responsabilidad aumentadas" cit. 12
[50] Durán Arroyo, A. "El nuevo reglamento de protección de datos personales. Análisis de su eficacia en la determinación de su ámbito territorial y los remedios en caso de tratamiento ilícito". *Revista Jurídica de la Universidad Autónoma de Madrid*, (37), 415-440 (p. 417)

se refiere a ellas como las que "han cambiado la concepción de la privacidad de los particulares, que exponen con menos reticencias aspectos de su vida privada que en otros contextos no expondrían y, vemos, por otro lado, el aumento de procedimientos, operaciones y transacciones realizados a través de Internet en el ámbito privado y en la relación de los ciudadanos con las administraciones públicas".[51]

Definitivamente, son el resultado del fenómeno de Internet. Constituyen "vías consolidadas de relación e interacción cotidianas, no sólo de las nuevas generaciones de adolescentes y jóvenes, sino también de todo el conjunto de nuestra sociedad"[52]. Según datos proporcionados por la Comisión Europea, las redes sociales tienen ya más de 270 millones de usuarios en todo el mundo, nueve de cada diez jóvenes afirman haber accedido a alguna de las redes sociales existentes y, ocho de cada diez jóvenes afirman tener su propia cuenta en alguna de ellas [53].

Aunque el nacimiento de las redes sociales data de finales de los años 90, y se consolidaron a partir de 2002[54], la verdadera revolución comenzó con el nacimiento de *Facebook* en 2005. Se creó por Mark Zuckerberg, dirigido inicialmente a universitarios residentes en Estados Unidos, y terminando por ser la mayor red social del mundo con cientos de millones de usuarios. Todos estos millones de usuarios se traducen en datos que comparten dichos usuarios en la red social. Se trata de un espacio virtual en el que los usuarios consumen información, pero a su vez ellos mismos aportan grandes cantidades de datos referentes a su esfera individual y personal.

En definitiva, es un fenómeno social que crece exponencialmente y es imparable, ello precisa que tenga una regulación adecuada ya que supone numerosos peligros, especialmente en el ámbito de la privacidad del individuo y de los derechos fundamentales del art. 18.1 y 18.4 CE, el peligro ha alcanzado tal magnitud que cada vez son más utilizadas como instrumento para el cibercrimen[55].

[51] "El nuevo reglamento de protección de datos personales. Análisis de su eficacia en la determinación de su ámbito territorial y los remedios en caso de tratamiento ilícito" cit. 417
[52] Gil Antón, A. M., "El fenómeno de las redes sociales y los cambios de vigencia de los derechos fundamentales", *Revista de Derecho UNED*, n.10, 2012, pp. 209-255, p. 209
[53] "El fenómeno de las redes sociales y los cambios de vigencia de los derechos fundamentales", cit. 213
[54] Redes como *My Space*, que apareció en 2003.
[55] "El fenómeno de las redes sociales y los cambios de vigencia de los derechos fundamentales", cit. 217

Estas características de la situación actual nos lleva a determinar que nos encontramos ante lo que denominamos una "sociedad de riesgo". Ello implica que esta nueva situación nos puede llevar a múltiples amenazas y peligros debido a su imparable evolución y no conseguimos regularla correctamente. Es decir, hay una preocupación tanto por parte de los legisladores como de los propios usuarios en lo referido a la efectividad del derecho a la protección de datos personales, ya que empiezan a tomar en consideración los posibles perjuicios que puede suponer la circulación de datos sin ningún tipo de control ni garantías.[56]

Sin embargo, esta preocupación por la privacidad ha podido pasar a un segundo plano dado que han surgido otras prioridades para las personas, tienen la necesidad de comunicarse constantemente dadas las herramientas que les proporcionan esa inmediatez para poder relacionarse, encontrar información, etc. Las aplicaciones de mensajería como *Whatsapp* nos permiten poder conectarnos en cualquier momento y lugar con cualquier persona del mundo. A pesar de que esto ha supuesto múltiples beneficios para la sociedad, también se han creado necesidades que anteriormente no teníamos ya que no era posible poder comunicarse de esa manera.

Dado el fácil acceso a estas plataformas digitales, resulta de especial relevancia mencionar la especial peligrosidad que supone para los menores de edad la participación en redes sociales. Si ya la mera participación en redes sociales entraña una serie de peligros para todos sus usuarios, si se trata de menores de edad, éstos se encontrarán ante una amenaza de mayor calibre. Aunque sea algo relativo, la falta de capacidad jurídica de obrar que establece el Código Civil se fundamenta en que aquellas personas que no hayan alcanzado la mayoría de edad todavía no han desarrollado ciertos aspectos de su personalidad y madurez que les permita realizar una serie de actividades.

Asimismo, cabe destacar un factor común en todas estas plataformas, su carácter gratuito, o al menos lo es de manera aparente. Ello ha sido una de las claves del éxito para que hayan podido formarse todas estas comunidades multitudinarias. Cabe plantearse qué beneficio obtienen las empresas creadoras de estas plataformas. Una primera respuesta en aplicaciones como *Instagram* o *Facebook* es la inclusión de publicidad dentro de las

[56] "El nuevo reglamento de protección de datos personales. Análisis de su eficacia en la determinación de su ámbito territorial y los remedios en caso de tratamiento ilícito", cit. 417

mismas. Sin embargo, debemos de ir más allá, porque quizás lo que realmente les proporciona un rendimiento positivo a las redes sociales es el tráfico de datos que les proporcionamos los propios usuarios a la plataforma. Por tanto ¿son verdaderamente gratuitas estas plataformas o realmente nosotros les estamos "regalando" multitud de datos que son objeto de un negocio posterior?. Esta cuestión debería de ser objeto de un profundo análisis por parte de la sociedad, pero resulta algo complejo llegar a este punto dado el poder que han adquirido las redes sociales.

En consecuencia, Internet se presenta como un espacio carente de fronteras, espaciales o temporales, con apariencia de gratuidad, donde la personalidad pasa a ser una personalidad social, pero donde además de generarse ventajas, se incrementan exponencialmente los riesgos del nacimiento de conductas lesivas, no sólo respecto la conculcación de los diversos derechos fundamentales a la intimidad, honor, la propia imagen o la protección de datos personales, sino también respecto de conductas ilícitas como el Ciberbullying[57].

3.4.2. Problemática del Consentimiento

El consentimiento siempre ha sido un concepto clave de la protección de datos, como un medio que permite respetar la autonomía de los individuos sobre la toma de sus decisiones.[58]

Ana María Gil Antón afirma que "en relación con la vida privada, uno de los mayores cambios que ha provocado el uso de las redes sociales, es el hecho de que la mayoría de la información personal que se publica en estos servicios se hace a iniciativa de los propios usuarios, con su propio consentimiento"[59]

La normativa relativa a la protección de datos, tanto en el ámbito europeo como en el español, inicialmente han considerado como principio determinante la prestación del consentimiento para la efectiva protección de datos personales.

[57] "El fenómeno de las redes sociales y los cambios de vigencia de los derechos fundamentales" cit. 251
[58] Gil González, E., *Big data, privacidad y protección de datos*, BOLETIN OFICIAL DEL ESTADO, Madrid, 2016 (p. 60)
[59] "El fenómeno de las redes sociales y los cambios de vigencia de los derechos fundamentales" cit. 228

Pero la realidad actual nos demuestra que no solo es necesario el consentimiento específico, sino que además se tiene que dar una mayor garantía de que el usuario de la red social tiene claramente conocimiento del tratamiento que se está haciendo con los datos que él mismo proporciona, para poder asegurar que la prestación de consentimiento es realmente inequívoca[60].

La ineficiencia del consentimiento nos demuestra que hay que tener en cuenta otros principios, como el de transparencia y responsabilidad demostrada para poder conseguir una protección efectiva para la persona, especialmente en lo relativo a sus derechos a la privacidad y a la protección de datos personales[61].

En definitiva, debemos de tener en cuenta más elementos aparte del consentimiento, ya que el planteamiento de que con el consentimiento es suficiente para que las plataformas digitales puedan eximirse de toda responsabilidad relativa al tratamiento que puedan hacer de los datos que sus usuarios les proporcionan ha quedado claramente obsoleta. Con esto queremos decir que hay que aumentar los mecanismos para poder exigir responsabilidad a los agentes encargados del tratamiento de datos en estas plataformas, para que no puedan eximir su responsabilidad con el mero consentimiento.

4. LA PROTECCIÓN DE DATOS PERSONALES

Antes de nada hay que exponer qué se entiende por dato de carácter personal, Elena Gil lo entiende como "cualquier información concerniente a personas físicas identificadas e identificables. Siendo una persona identificable cuando su identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social, salvo que dicha identificación requiera actividades o plazos desproporcionados."[62]

[60] Informe Jurídico de la Agencia Española de Protección de Datos 93/2008, sobre "Formas de obtener el consentimiento mediante Web. Conocimiento tácito".
[61] "*Big Data*: Hacia la protección de datos personales basada en una transparencia y responsabilidad aumentadas" cit. 9
[62] "*Big data, privacidad y protección de datos*" cit. 45

El *big data* tiene implicaciones para la protección de datos personales y la privacidad. El derecho a la protección de datos personales es un derecho específico, en el sentido de autónomo, que surge a partir del derecho a la intimidad[63]. Efectivamente, el *big data* puede representar un reto para diferentes cuerpos normativos, tales como la protección de datos, la prohibición de la discriminación, el derecho de la competencia, etc. El tema que nos concierne son los problemas sobre la privacidad y la protección de datos.

Tal y como establece el reglamento de protección de datos en su considerando cuarto, el tratamiento de datos personales debe estar concebido para servir a la humanidad El derecho a la protección de los datos personales no es un derecho absoluto sino que debe considerarse en relación con su función en la sociedad y mantener el equilibrio con otros derechos fundamentales, con arreglo al principio de proporcionalidad[64]

Debido a los riesgos que han sido citados en el anterior apartado, hay que plantearse cómo se protegerán los datos personales y la privacidad en la era de los datos personales y tratamientos masivos.

El objeto de esta protección, tal y como recoge la LOPD es "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 intimidad personal y familiar"[65]

Como señalábamos anteriormente, la normativa de protección de datos se aplica cuando la información de las personas físicas hace que éstas sean identificadas o identificables. Por consiguiente, "cuando los datos no hacen identificable a una persona, no se aplica esta regulación"[66].

Aunque el derecho a la protección de datos está íntimamente relacionado con el derecho a la privacidad, ya hemos mencionado que es un derecho de carácter autónomo que atribuye al titular "un poder de disposición sobre sus propios datos personales; esto es, un poder que abarca desde el derecho del afectado a que se solicite su previo

[63] "*Big Data*: Hacia la protección de datos personales basada en una transparencia y responsabilidad aumentadas" cit. 10
[64] Considerando cuarto Reglamento (UE) 2016/679, de 27 de abril de 2016, de Protección de datos
[65] "*Big data, privacidad y protección de datos*" cit.50
[66] "*Big data, privacidad y protección de datos"* cit. 51

consentimiento para recoger y usar sus datos personales, hasta su derecho a ser informado sobre el destino de estos y a acceder, rectificar y cancelar dichos datos"[67].

Como explicábamos en el anterior apartado, la realidad actual nos ha llevado a la denominación de la "sociedad de riesgo". En este sentido, tal y como señala Minero Alejandre, a partir del Eurobarómetro 2015, vemos una creciente concienciación sobre el valor de los datos personales y las políticas de privacidad.[68]

4.1. Impacto del Big Data en la normativa de protección de datos

El *big data* puede suponer un desafío para diferentes cuerpos normativos, como el de protección de datos. Como se ha dicho la normativa de protección de datos personales se aplica cuando la información analizada hace que las personas físicas que son titulares de dicha información sean identificadas o identificables.

Por otra parte, cuando los datos analizados no identifican o hacen identificable a una persona, no se aplicará esta regulación. Para poner solución, se han creado una serie de técnicas para que estos datos no puedan identificar a sus titulares, tales como la anonimización o el proceso de disociación

Por un lado, la anonimización tiene como objetivo poder proteger la privacidad de los individuos titulares de los datos analizados, convirtiendo los datos en no personales. En este caso no sería aplicable ninguna normativa de protección de datos al no verse éstos desprotegidos.[69]

Con respecto al proceso de disociación, también llamado seudonimización en el tratamiento de datos personales, cuyo objetivo es que la información que se obtenga de los datos no pueda asociarse a una persona identificada o identificable.[70] Este procedimiento se lleva a cabo antes de que se acceda y traten los datos, si se cumplía con estas prerrogativas, eximía del cumplimiento de las obligaciones establecidas en la Ley Orgánica vigente en aquel momento.

---

[67] Durán Arroyo, A. "El nuevo reglamento de protección de datos personales. Análisis de su eficacia en la determinación de su ámbito territorial y los remedios en caso de tratamiento ilícito". *Revista Jurídica de la Universidad Autónoma de Madrid*, (37), 415-440. Pag 416

[68] Minero Alejandre, G., "Presente y futuro de la protección de datos personales. Análisis normativo y jurisprudencial desde una perspectiva nacional y europea" *Anuario jurídico y económico escurialense*, n. 50, 2017, pp.13-58 p.15

[69] "*Big data, privacidad y protección de datos"* cit. 51

[70] Artículo 3 de La Ley Orgánica 15/1999 de Protección de Datos

Teniendo en cuenta que nuestra realidad virtual hace que se produzca una evolución rápida, constante e imparable del *big data*, esta situación supone un desafío para la normativa de protección de datos ya que facilita la re-identificación de los sujetos, ya no solo a partir de los datos disociados, sino también a partir de los datos que considerábamos anónimos. En otras palabras, las técnicas de anonimización y disociación de los datos han dejado de ser suficientes con la llegada del *big data*.[71]

Efectivamente, Recio Gayo subraya esta afirmación añadiendo que aun así "sigue siendo útil como una protección adicional, pero no es robusta para el futuro próximo de los métodos de re-identificación"[72]. Lo dicho hasta aquí supone que en la actualidad la anonimización supone un *plus* o valor añadido para la privacidad y la protección de datos personales, pero no la técnica que solucione de manera definitiva e infalible el problema de re-identificación de los sujetos titulares de los datos[73].

Elena Gil sintetiza de manera adecuada cuáles han sido los retos principales que ha supuesto el progreso de las tecnologías de la información, concretamente el *big data*, para las normas de protección de datos personales y que han impulsado la reforma de la Directiva que era vigente hasta hace un año.

En primer lugar, la Directiva no ha podido adaptarse al entorno tecnológico ya que cuando ésta fue promulgada, en 1995, apenas había comenzado el amplio desarrollo que ha supuesto Internet. Al mismo tiempo, no se había dado una implementación efectiva del principio de minimización de datos, es decir, que los datos recopilados no fueran excesivos.

Asimismo, la Directiva reflejaba excesiva confianza en el consentimiento informado del individuo para poder recopilar y tratar sus datos de carácter personal. Por otro lado, las técnicas de anonimización ha demostrado tener limitaciones y no ser suficientes con los nuevos avances tecnológicos, ahora es mucho más sencillo poder re-identificar a los sujetos.

[71] "*Big data, privacidad y protección de datos*" cit. 52
[72] "*Big Data*: Hacia la protección de datos personales basada en una transparencia y responsabilidad aumentadas" cit. 20
[73] "*Big Data*: Hacia la protección de datos personales basada en una transparencia y responsabilidad aumentadas" cit. 20

Por último. El *big data* aumenta el riesgo de toma de decisiones de forma automática, ello implica que decisiones relevantes en nuestra vida tengan que depender de algoritmos que se ejecutan de manera automática.[74]

4.2. Normativa en el ámbito europeo y nacional

Mientras que el apartado segundo de este trabajo lo dedicábamos a explicar los motivos por los que este derecho tiene una particular protección como derecho fundamental, a nivel europeo (reflejado en la Carta de Derechos Fundamentales de la UE y en el Tratado de Funcionamiento de la UE), en este apartado vamos a centrarnos en la normativa que regula la protección de datos, tanto a nivel europeo como a nivel nacional.

Durán Arroyo afirma que "el poder de disposición es otorgado por la normativa que desarrolla la protección de datos, a través de los mecanismos necesarios para garantizar al titular una defensa y protección adecuadas frente a operaciones sobre sus datos, manuales o automatizadas, que por incumplimiento de la normativa no sean respetuosas con este derecho"[75].

La regulación de estas garantías es especialmente compleja y, además, una cuestión de plena actualidad jurídica tras haber sido la reforma de la normativa esencial en esta materia en el ámbito de la Unión Europea.

4.2.1. Ámbito europeo

Dado que resulta extremadamente complejo abordar un análisis global, nos centraremos en la legislación de la Unión Europea (UE), "por ser el ámbito de mayores progresos en términos de armonización normativa, dirigida a asegurar tanto los derechos de los titulares como la libre circulación de datos en la formación del mercado único"[76].

[74] "*Big data, privacidad y protección de datos*" cit. 53
[75] "El nuevo reglamento de protección de datos personales. Análisis de su eficacia en la determinación de su ámbito territorial y los remedios en caso de tratamiento ilícito" cit. 416
[76] "El nuevo reglamento de protección de datos personales. Análisis de su eficacia en la determinación de su ámbito territorial y los remedios en caso de tratamiento ilícito" cit. 418

Cabe recordar que a nivel europeo, la protección de datos está configurada como un derecho fundamental (recogido en el art. 16 TFUE y el art. 8 de la Carta de Derechos Fundamentales de la Unión Europea).

En 1980 se publicaron las Directrices de Privacidad de la Organización para la Cooperación y el Desarrollo Económicos (OCDE), y en 1981 el Consejo de Europa adoptó el Convenio nº 108 para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal, que era el único instrumento internacional vinculante sobre protección de datos en aquel momento[77].

Todas estas normas dieron lugar a la **Directiva 95/46/CE** del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. El objetivo de esta Directiva era "regular el equilibrio que debe existir entre la protección de la vida privada de las personas físicas y la libre circulación de datos personales dentro de la Unión Europea"[78]. En otras palabras, la Directiva buscaba la protección en particular del derecho a la intimidad en las personas físicas[79].Todavía cabe recalcar que lo que trataba de hacer la Directiva era armonizar la protección de los derechos y las libertades fundamentales de las personas físicas en relación con las actividades de tratamiento de datos de carácter personal y garantizar la libre circulación de estos datos entre los Estados miembros de la Unión Europea[80].

La Directiva "fue el principal instrumento jurídico aplicable al mercado interior, transpuesto en los Estados miembros y en el Espacio Económico Europeo (Noruega, Islandia y Liechtenstein)"[81]

Sin embargo, con el paso del tiempo se apreciaron en la Directiva una serie de carencias y defectos de contenido ya que "no estaba adaptada a la realidad social y jurídica que supone Internet y por las dudas que suscitaban algunos preceptos, como el relativo al ámbito territorial; el alcance de la uniformización jurídica era limitado dada la necesaria transposición de la

[77] "*Big data, privacidad y protección de datos*" cit. 49
[78] "*Big data, privacidad y protección de datos*" cit. 49
[79] Artículo 1 de la Directiva 95/46/CE
[80] Considerando tercero del Reglamento (UE) 2016/679, de 27 de abril de 2016, de Protección de datos
[81] "El nuevo reglamento de protección de datos personales. Análisis de su eficacia en la determinación de su ámbito territorial y los remedios en caso de tratamiento ilícito" cit. 418

normativa en cada uno de los Estados Miembros" [82]. Todo esto ha llevado finalmente a una modificación legislativa.

"Aunque los objetivos y principios de la Directiva 95/46/CE siguen siendo válidos, ello no ha impedido que la protección de los datos en el territorio de la Unión Europea se aplique de manera fragmentada, ni la inseguridad jurídica ni una percepción generalizada entre la opinión pública de que existen riesgos importantes para la protección de las personas físicas, en particular del derecho a la protección de los datos de carácter personal. Hay diferencias en los niveles de protección debido a las diferencias en la ejecución y aplicación de la Directiva"[83]

Fue en el año 2012 cuando la Comisión Europea decidió abordar una reforma aplicando así el artículo 33 de la Directiva[84]. Hasta que fue tomada dicha decisión, había sido el Tribunal de Justicia de la Unión Europea (TJUE) el que había ido colmando las lagunas contenidas en la Directiva.

El objetivo que tenía la Comisión Europea con esta reforma era una modernización de los principios originarios de este derecho, así como establecer un marco legal y único para toda la UE que partiera de las mismas fuentes jurídicas de la Directiva.[85]En otras palabras, la Propuesta de la Comisión mantenía los objetivos y principios sobre la protección de datos introduciendo cambios en su aplicación para así adaptarse a la realidad tecnológica actual. Entre los principales cambios perseguidos se encontraban nuevos derechos de privacidad (el derecho al olvido y la portabilidad de datos), el endurecimiento de los deberes de transparencia, reforzar la importancia del consentimiento.[86]

Tras varios años de elaboración, finalmente el 27 de abril de 2016 tuvo lugar la adopción del resultado de dicha reforma, que ha sido el **Reglamento 2016/679** del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (en adelante, **Reglamento General de Protección de Datos**) y por el que se deroga la Directiva 95/46/CE. Hay que señalar que este Reglamento es el resultado de varios años de debate entre los diferentes organismos, instituciones y autoridades de

[82] "El nuevo reglamento de protección de datos personales. Análisis de su eficacia en la determinación de su ámbito territorial y los remedios en caso de tratamiento ilícito" cit. 419
[83] Considerando octavo del Reglamento 2016/679 de Protección de datos
[84] Sobre la presentación de propuestas necesarias en función de los avances de la tecnología de la información, y a la luz de los trabajos de la sociedad de información.
[85] "El nuevo reglamento de protección de datos personales. Análisis de su eficacia en la determinación de su ámbito territorial y los remedios en caso de tratamiento ilícito" cit. 419
[86] " *Big data, privacidad y protección de datos*" cit. 54

protección de datos europeas y las empresas. Reiteramos que ha la decisión de la modificación legislativa ha sido fruto del incesante avance de las nuevas tecnologías de la información en las últimas décadas debiendo adaptarse a las nuevas necesidades para proporcionar el derecho a la privacidad y la protección de datos[87].

El Reglamento comenzó a ser aplicable el 25 de mayo de 2018, éste tiene una serie de objetivos tales como "la unificación normativa, poder mejorar la regulación para acabar así con la fragmentación de los instrumentos jurídicos en el territorio de la UE, para así garantizar una mayor seguridad jurídica tanto para los titulares de los derechos como para responsables y encargados del tratamiento"[88].
Asimismo, tenemos la **Corrección de errores** de este Reglamento General de protección de datos.[89]

4.2.2. Ámbito nacional

En el ordenamiento jurídico español, la protección de datos personales fue desarrollada por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter Personal (la LOPD), y su Reglamento de desarrollo, aprobado mediante Real Decreto 1720/2007, de 21 de diciembre (el denominado Reglamento General de Protección de datos)
También existían otras normas sectoriales como la Ley 34/2002, de 11 de julio, de servicios de la Sociedad de la Información y de Comercio Electrónico o la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.

Sin embargo, la legislación ha sido objeto de reforma como consecuencia de los cambios en la normativa en el ámbito de la Unión Europea.

[87] Alarcón Caparrós, V., "GDPR: ¿qué necesitas saber del nuevo Reglamento Europeo de Protección de Datos?"*Signaturit*, 2018 (disponible en https://blog.signaturit.com/es/las-claves-sobre-el-nuevo-reglamento-europeo-de-proteccion-de-datos)
[88] "El nuevo reglamento de protección de datos personales. Análisis de su eficacia en la determinación de su ámbito territorial y los remedios en caso de tratamiento ilícito" cit. 419
[89] Agencia española de Protección de datos: https://www.aepd.es/normativa/index.html

A pesar de que el Reglamento 2016/679 tiene aplicación directa en todos los Estados miembros de la Unión Europea incluyendo los casos en que los Estados Miembros no hayan transpuesto dicho Reglamento. El contenido del Reglamento es el mismo en todos los Estados miembros de la Unión Europea. Conviene señalar que el propio Reglamento establece que sus normas deben ser especificadas por los Derechos de los Estados miembros. En la medida en que sea necesario por razones de coherencia y para que las disposiciones nacionales sean comprensibles para sus destinatarios, pueden incorporar a su derecho nacional elementos del Reglamento.[90]

Por consiguiente, en la actualidad nos encontramos con la **Ley Orgánica 3/2018**, **de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales**. No obstante, las normas sectoriales anteriormente citadas continúan siendo referencia actualmente.[91]

Por último, cabe destacar también la **Circular 1/2019**, de 7 de marzo, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales relativos a opiniones políticas y envío de propaganda electoral por medios electrónicos o sistemas de mensajería por parte de partidos políticos, federaciones, coaliciones y agrupaciones de electores al amparo del artículo 58 bis de la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General.

La legislación española en materia de protección de datos es aplicable en los siguientes casos:

1) Cuando el tratamiento de los datos se realiza en territorio español en el marco de las actividades propias de un establecimiento del que sea titular el responsable del tratamiento de los datos
2) Cuando el responsable del tratamiento de los datos no está establecido dentro del territorio español, pero le es aplicable la legislación española conforma a las normas de Derecho Internacional Público.

[90] Considerando octavo del Reglamento 2016/679, de 27 de abril de 2016, de Protección de Datos
[91] Agencia española de Protección de datos: https://www.aepd.es/normativa/index.html

3) Cuando el responsable del tratamiento de los datos no está establecido en ningún país de la Unión Europea, pero en el tratamiento de los datos utiliza medios situados en territorio español, salvo que tales medios se utilicen únicamente con fines de tránsito.[92]

El **ámbito de aplicación** de la Ley Orgánica 3/2018 es el siguiente[93]:

"*Se aplicará a cualquier tratamiento total o parcialmente de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero*"

Se **excluye** de dicho ámbito de aplicación[94]:

"*a) A los tratamientos excluidos del ámbito de aplicación del Reglamento general de protección de datos por su artículo 2.2, sin perjuicio de lo dispuesto en los apartados 3 y 4 de este artículo.*

b) A los tratamientos de datos de personas fallecidas, sin perjuicio de lo establecido en el artículo 3.

c) A los tratamientos sometidos a la normativa sobre protección de materias clasificadas."

"*Los tratamientos a los que no sea directamente aplicable el Reglamento (UE) 2016/679 por afectar a actividades no comprendidas en el ámbito de aplicación del Derecho de la Unión Europea, se regirán por lo dispuesto en su legislación específica si la hubiere y supletoriamente por lo establecido en el citado reglamento y en la presente ley orgánica. Se encuentran en esta situación, entre otros, los tratamientos realizados al amparo de la legislación orgánica del régimen electoral general, los tratamientos realizados en el*

[92] "*Big data, privacidad y protección de datos*" cit. 50
[93] Artículo 2.1 de la Ley Orgánica 3/2018 de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales
[94] Artículo 2.2 de la Ley Orgánica 3/2018 de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales

ámbito de instituciones penitenciarias y los tratamientos derivados del Registro Civil, los Registros de la Propiedad y Mercantiles".[95]

"*El tratamiento de datos llevado a cabo con ocasión de la tramitación por los órganos judiciales de los procesos de los que sean competentes, así como el realizado dentro de la gestión de la Oficina Judicial, se regirán por lo dispuesto en el Reglamento (UE) 2016/679 y la presente ley orgánica, sin perjuicio de las disposiciones de la Ley Orgánica 6/1985, de 1 julio, del Poder Judicial, que le sean aplicables*".[96]

4.3. Similitudes entre la Directiva y el Reglamento de protección de datos

Ya se ha mencionado que la propuesta que tenía la Comisión Europea al plantear la reforma de la normativa en 2012 tenía los mismos objetivos de la Directiva. Esto es, tanto la Directiva como el Reglamento actual de protección de datos comparten el mismo objeto, que es proteger los derechos y libertades de los sujetos titulares, estableciendo criterios fundamentales que permitan calificar como lícito un tratamiento un tratamiento de datos por parte de responsables y encargados[97]

Además, ambos textos normativos comparten el ámbito espacial de aplicación de la legislación europea sobre protección de datos, ello determina en qué situaciones los responsables del tratamiento de datos, incluyendo terceros Estados, deben cumplir con las obligaciones y quedan sometidos a la supervisión de las autoridades de control[98]

Asimismo, el actual Reglamento mantiene el modelo de protección implantado por la Directiva y no rompe con la jurisprudencia asentada del TJUE. Alicia Durán concluye acertadamente que el Reglamento actual de protección de datos "tiene como **base** la continuidad de los principios que conforman el contenido esencial del derecho a la

[95] Artículo 2.3 de la Ley Orgánica 3/2018 de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales
[96] Artículo 2.4 de la Ley Orgánica 3/2018 de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales
[97] Responsable es aquella persona física o jurídica que decide los fines y medios del tratamiento (art. 2.d) Directiva y 4.7 RPD). El encargado trata los datos por cuenta del responsable (2.e) Directiva y art. 4.8 RPD). Mientras que la Directiva solo atribuía obligaciones al responsable, el nuevo Reglamento de Protección de Datos reconoce también obligaciones del encargado de las que corresponde directamente.
[98] De Miguel Asensio, P. A., "Competencia y derecho aplicable en el Reglamento General de Protección de Datos de la Unión Europea" *Revista Española de Derecho Internacional*, vol. 69/1, 2017, Madrid, pp.75-108, p. 78

protección de datos. Partiendo de esta base, su **finalidad** es garantizar la coherencia y uniformidad en una regulación de aplicación estricta, así como el desarrollo económico en el mercado interior y el otorgamiento de un mayor control a los ciudadanos sobre sus derechos y mayor seguridad jurídica y práctica"[99].

Por otro lado, tanto el significado del tratamiento como el ámbito de aplicación material es esencialmente el mismo (Art. 3 de la Directiva y art. 2 RPD)[100].

En consonancia con Alicia Durán Arroyo, para que el tratamiento de datos sea acorde al ámbito material del derecho de la Unión Europea[101], este deberá de ser lícito en los términos de la norma, para proteger los derechos de los titulares.

Sin embargo, ninguno de los dos textos tiene aplicación universal, por lo que cabe plantearse cuándo quedan responsables y encargados sujetos al Derecho de la Unión Europea. Aquí entran en juego los artículos 4 de la Directiva y 3 del Reglamento de Protección de Datos, que comparten la función de determinar el ámbito de aplicación territorial de la normativa europea[102].

4.4 Cambios introducidos en el Reglamento 2016/679

En este apartado vamos a desarrollar las modificaciones efectuadas en la normativa vigente en el ámbito de la UE de protección de datos personales. El nuevo Reglamento presenta una transformación de la situación basada en la armonización.

En primer lugar, mientras que en la Directiva el artículo 4 tiene una doble función: por un lado, determina en qué supuestos será aplicable el cuerpo normativo; y por otro lado, establece cuál es el Estado Miembro que deberá aplicar su ley nacional fruto de la transposición de la normativa europea[103]. Sin embargo, el Reglamento de Protección de Datos elimina esta segunda función, ya que este cuerpo normativo va a ser el mismo para

[99] "El nuevo reglamento de protección de datos personales. Análisis de su eficacia en la determinación de su ámbito territorial y los remedios en caso de tratamiento ilícito" cit. 420
[100] Todo tipo de operaciones realizadas sobre los datos, desde su recogida hasta su gestión, proceso o cesión a un tercero (art. 2.b) Directiva y art. 4.2 RPD)
[101] Tratamiento total o parcialmente automatizado de datos personales, así como el tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero (art. 3.1 Directiva y art. 2.1 RPD)
[102] "El nuevo reglamento de protección de datos personales. Análisis de su eficacia en la determinación de su ámbito territorial y los remedios en caso de tratamiento ilícito" cit. 421
[103] Artículo 4 de la Directiva 95/46/CE

todos los Estados Miembros, a pesar de que sigan teniendo la posibilidad de regular algunas cuestiones[104]. En otras palabras, se trata de un cambio de instrumento normativo, ya que frente a las deficiencias que tenía la Directiva tales como la fragmentación del entorno causando así inseguridad jurídica, en el Reglamento se ha apostado por la unificación para así sustituir a las legislaciones nacionales, salvo en los casos en que el Reglamento prevea que sus normas puedan ser especificadas o restringidas por los Estados miembros, como observa en su artículo octavo sobre la edad aplicable al consentimiento de los niños[105].

En segundo lugar, el Reglamento ofrece novedades muy significativas en el ámbito internacional. Por regla general, tras la labor de unificación normativa del Reglamento no será necesario en las situaciones intracomunitarias determinar la legislación de qué Estado miembro es aplicable respecto a las materias del Reglamento[106].

Una de las principales diferencias entre Reglamento y Directiva se refleja cuando se da la situación en la que el responsable no tenga un establecimiento en el territorio de algún Estado Miembro de la Unión. Es decir, aquellos supuestos en los que resulte de aplicación el Derecho de la UE aunque el responsable se encuentre fuera de su ámbito territorial[107]:

Por un lado, podemos destacar una función común con respecto a la delimitación del ámbito territorial de aplicación de la legislación de la Unión, reflejado en el artículo 4.1 de la Directiva y el artículo 3 del Reglamento, ambos cuerpos normativos recogen condiciones o conexiones necesarias para poder entablar dentro de su ámbito de aplicación a nivel europeo la conducta de un individuo que se encuentra fuera de su ámbito territorial.

Mientras que en la Directiva, esa conexión necesaria es la utilización de *medios*[108] (no con meros fines de tránsito) situados en el territorio europeo. Esta previsión fue fuertemente criticada por su amplitud por el GT29, ya que podría llevar a supuestos de

[104] Considerando octavo del Reglamento 2016/679, de 27 de abril de 2016, de Protección de Datos
[105] "Competencia y derecho aplicable en el Reglamento General de Protección de Datos de la Unión Europea" cit. 77
[106] "Competencia y derecho aplicable en el Reglamento General de Protección de Datos de la Unión Europea" cit. 77
[107] "El nuevo Reglamento de Protección de Datos Personales. Análisis de su eficacia en la determinación de su ámbito territorial y los remedios en caso de tratamiento ilícito" cit. 423
[108] Hay una amplia interpretación del criterio *medios* que "incluye intermediarios y/o técnicos tales como las muestras o encuestas. En consecuencia, se aplica a la recogida de información mediante cuestionarios, como ocurre, por ejemplo, en algunas pruebas farmacéuticas" (GT29, Dictamen 8/2010 sobre el Derecho aplicable, cit., p.23)

conexión con la normativa europea en casos en que apenas hay conexión con la Unión Europea[109]. En definitiva, esta previsión "podría derivar en prácticamente una aplicación universal de la normativa que en realidad no tiene"[110].

Para paliar esto, el Reglamento de Protección de Datos incluye dos condiciones que operarán como lazos de conexión en el supuesto de los responsables que se encuentren fuera de la Unión:

- El tratamiento debe ser sobre datos que se encuentren en la Unión Europea. Aunque el texto literal en su versión española recoge la expresión de "residente de la Unión Europea", un análisis comparado del texto en otros idiomas nos lleva a la conclusión de que su voluntad no se limita a residentes en la Unión[111].

- Dicho tratamiento debe dirigir una oferta de bienes y servicios así como controlar su comportamiento[112].

El Reglamento moderniza así la normativa con la inclusión de supuestos como el "uso de cookies y otros archivos informáticos que permiten el acceso a información en el equipo del usuario"[113], así como la actividad de empresas que utilizan información sobre el comportamiento para fines comerciales y publicitarios. Exigiendo el nombramiento de un representante en la Unión que actúe como contacto con Autoridades y ciudadanos[114].

El asunto *Google Spain* demuestra que, con las novedades introducidas en el Reglamento en este aspecto, los lazos de conexión con la Unión quedan clarificados y se otorga una mayor seguridad jurídica para la aplicación de la normativa europea en caso de que el responsable no se encuentre en el territorio de la UE, porque ya no se basan en la condición del uso de medios ubicados en el territorio como ocurría en la Directiva[115].

[109] Como puede suceder en el caso de que un responsable solo utilice los medios ubicados en el territorio de la Unión Europea pero sin realizar tratamiento en el mismo ni sobre sus residentes.
[110] "El nuevo Reglamento de Protección de Datos Personales. Análisis de su eficacia en la determinación de su ámbito territorial y los remedios en caso de tratamiento ilícito" cit. 423
[111] "Competencia y derecho aplicable en el Reglamento General de Protección de Datos de la Unión Europea" cit. 83
[112] El nuevo Reglamento de Protección de Datos Personales. Análisis de su eficacia en la determinación de su ámbito territorial y los remedios en caso de tratamiento ilícito" cit. 424
[113] "Competencia y derecho aplicable en el Reglamento General de Protección de Datos de la Unión Europea" cit. 86
[114] El nuevo reglamento de protección de datos personales. Análisis de su eficacia en la determinación de su ámbito territorial y los remedios en caso de tratamiento ilícito" cit. 424
[115]"El nuevo reglamento de protección de datos personales. Análisis de su eficacia en la determinación de su ámbito territorial y los remedios en caso de tratamiento ilícito" cit. 425

A pesar de las mejoras en este aspecto, aclarando así la aplicación de la norma, "no se han conseguido superar las críticas sobre una posible extensión global y extraterritorial de la legislación de la Unión Europea" [116].

4.5. Remedios en caso de tratamiento ilícito

El artículo 77.1 del Reglamento de Protección de Datos establece el derecho de todo interesado a presentar una reclamación ante una autoridad de control si considera que el tratamiento de sus datos infringe lo establecido en el propio Reglamento.[117]

Si el sujeto titular de la información o datos desea reclamar por su aparente trato ilícito, puede acudir a diferentes vías: Por un lado, cuenta con una tutela administrativa ante las autoridades de control, cuya actuación puede ser reclamable en vía judicial. Por otro lado, puede dirigirse contra el propio responsable del tratamiento y, en caso del Reglamento de Protección de Datos, contra los encargados.

4.5.1. Tutela Administrativa ante las autoridades de control

Procede comenzar resaltando que con los cambios introducidos en el Reglamento de Protección de Datos, las autoridades de control, como "guardianas de los derechos relacionados con el tratamiento de datos personales"[118], que están establecidas en todos los Estados Miembros de la Unión, han sido dotadas de un mayor número de competencias y funciones por el Reglamento. A partir del asunto *Schrems*[119] pueden apreciarse claramente estos cambios.

[116] "El nuevo reglamento de protección de datos personales. Análisis de su eficacia en la determinación de su ámbito territorial y los remedios en caso de tratamiento ilícito" cit. 425
[117] "Competencia y derecho aplicable en el Reglamento General de Protección de Datos de la Unión Europea" cit. 91
[118] Sentencia del Tribunal de Justicia de la Unión Europea C-518/07 de 9 de marzo de 2010 (Diario Oficial de la Unión Europea, 1 de mayo de 2010).Párr.23
[119] Sentencia del Tribunal de Justicia de la Unión Europea C-362/14, de 6 de octubre de 2015, *Schrems*, (Diario Oficial de la Unión Europea, 6 de octubre de 2015)

El nuevo Reglamento introduce cambios en la jurisdicción en lo relativo al ámbito de competencias y poderes que ostentas las autoridades de control, ya que se elimina la correlación de ley nacional y competencia como resultado de la unificación normativa característica del nuevo cuerpo normativo. En otras palabras, el ámbito de actuación y competencias ya no se limita exclusivamente al Estado Miembro al que pertenecen[120]. Ahora bien, las autoridades de control mantienen la competencia para desempeñar las funciones que se le asignen y ejercer los poderes que se le confieran en el territorio de su Estado Miembro[121], también se contempla el caso de que la autoridad de control de un Estado Miembro pueda actuar en el territorio de otro Estado Miembro.

Esto último resultará especialmente relevante para los **tratamientos transfronterizos** de datos[122] dentro del territorio de la Unión Europea, como sucede en el asunto *Schrems*. Según lo establecido en el Reglamento se dan dos clases de tratamientos transfronterizos:

- "Que el tratamiento de datos se realiza en el contexto de las actividades de un establecimiento de un responsable o encargado de la Unión Europea y el responsable o encargado está establecido en más de un Estado Miembro.
- O bien el tratamiento de datos tiene lugar en el contexto de las actividades de un único establecimiento de un responsable o encargado afecta o es probable que afecte sustancialmente a interesados en más de un Estado Miembro (asunto *Schrems*)[123]

Las decisiones de las autoridades de control son objeto de recursos administrativos y eventualmente ante tribunales de lo contencioso-administrativo.

4.5.2.Tutela civil contra los responsables o encargados

El art. 79 del Reglamento de Protección de Datos regula la tutela judicial contra un responsable o encargado del tratamiento, que deviene especialmente relevante respecto

[120] Sentencia del Tribunal de Justicia de la Unión Europea C-230/14, de 1 de octubre de 2015, *Weltimmo* (párr. 57)
[121] Artículo 56.2 del Reglamento 2016/679, de 27 de abril de 2016, de Protección de Datos
[122] Artículo 4.23 del Reglamento 2016/679, de 27 de abril de 2016, de Protección de Datos
[123] "El nuevo Reglamento de Protección de Datos Personales. Análisis de su eficacia en la determinación de su ámbito territorial y los remedios en caso de tratamiento ilícito" cit. 427

al derecho de toda persona que sufra daños y perjuicios a recibir una indemnización, como consecuencia de la infracción del Reglamento[124].

Mientras que una reclamación ante la autoridad de control no permite obtener la reparación del daño, esta tutela civil nos proporciona el derecho a indemnización. El Reglamento no introduce mecanismos de coordinación entre la tutela judicial civil y la supervisión administrativa, aunque la Propuesta de la Directiva sí lo contemplase[125].

El ejercicio de las acciones judiciales frente a los sujetos que han vulnerado sus derechos (responsables o encargados) como consecuencia de un tratamiento ilícito de datos personales da lugar a litigios ante los tribunales del orden civil (salvo que el responsable o encargado sea una administración pública).[126]

Además del derecho de indemnización, también pueden ejercitarse ante el orden jurisdiccional civil otro tipo de acciones fundadas en la infracción del Reglamento de Protección de Datos, como la imposición al responsable de una limitación o prohibición al tratamiento.

El Reglamento introduce como novedad la previsión de una norma especial de competencia judicial internacional en materia civil. Su art. 79.2 atribuye a los interesados que consideren que sus derechos han sido vulnerados la posibilidad de demandar al responsable o al encargado del tratamiento ante los tribunales de cualquier Estado en el que tengan un establecimiento, asimismo contempla que puedan demandar ante los tribunales de su propia residencia habitual[127].

Se trata de acciones civiles (salvo que el responsable sea una administración pública) que se encuentran en el ámbito de aplicación del Reglamento de Bruselas I Bis, ya que no se refieren a ninguna de las materias excluidas conforme a su art. 1.2. Por ello, la interacción entre el art. 79.2 del Reglamento de Protección de Datos y el Reglamento de Bruselas I Bis reviste particular interés[128].

[124] Artículo 82 del Reglamento 2016/679, de 27 de abril de 2016, de Protección de Datos
[125] "Competencia y derecho aplicable en el Reglamento General de Protección de Datos de la Unión Europea" cit. 92
[126] "Competencia y derecho aplicable en el Reglamento General de Protección de Datos de la Unión Europea" cit. 92
[127] Situaciones delimitadas por el art. 79.1 del Reglamento de Protección de Datos
[128] "Competencia y derecho aplicable en el Reglamento General de Protección de Datos de la Unión Europea" cit. 95

5.**CONCLUSIONES**

El cambio que supuso el *big data* ha conllevado una serie de circunstancias y hechos que eran imprevisibles, que no sólo han generado unas ventajas indudables en el ámbito de las relaciones humanas, suprimiendo así fronteras espaciales y temporales, sino también la existencia de peligros y amenazas para la privacidad del individuo, cuyo impacto de futuro no se ha podido todavía evaluar. (De Miguel Asensio, pag 250)

El *Big Data* y, concretamente, las redes sociales han supuesto una amenaza para la efectiva protección de los derechos fundamentales de protección de datos personales e intimidad. Por ello, se motivó una modificación en la normativa para intentar paliar los problemas que habían surgido. Por lo tanto, debemos de preguntarnos si el actual Reglamento ha solucionado todos los peligros e inconvenientes.

Por un lado, es una evidencia que el Reglamento de Protección de Datos supone un importante avance en la protección de datos respecto a la Directiva, ya que ha modernizado su contenido, aumentado la certidumbre y la seguridad jurídica gracias a la armonización, eliminando así los problemas que surgían en la Directiva por su uniformización jurídica limitada.

Sin embargo, hay parte de este objetivo que no se ha conseguido, ya que los responsables y encargados del tratamiento de datos deben seguir enfrentándose a materias que dentro del Reglamento debe regular cada Estado Miembro, que es precisamente lo que se pretendía evitar. Además, ello implica que habrá diferencias en la protección de los titulares según el territorio en dichas materias.[129]Esta situación se ve agravada por la falta de previsión de su relación con otros instrumentos y ramas del Derecho.

En definitiva, el nuevo Reglamento de Protección de Datos ha sido una primera aproximación, que era reclamada con urgencia, para poder llegar a una regulación que tenga como uno de sus fundamentos principales el fortalecimiento de una verdadera protección de datos en la que se consiga un equilibro entre el desarrollo de las nuevas realidades tecnológicas y la defensa de un derecho fundamental como es la protección de datos.

[129] "El nuevo Reglamento de Protección de Datos Personales. Análisis de su eficacia en la determinación de su ámbito territorial y los remedios en caso de tratamiento ilícito" cit. 435

También hay que decir que este Reglamento es un instrumento que deberá ser objeto de reforma, ya que tendrá que adaptarse constantemente a una sociedad que no deja de innovar y avanzar tecnológicamente, a tal ritmo que el legislador debe necesariamente adecuarse y anticiparse para así evitar situaciones irreversibles.
Por lo tanto, para poder conseguir una normativa europea de protección de datos real y efectiva todavía requiere mucho trabajo en el futuro "y será de nuevo la práctica jurídica la que a través de la jurisprudencia señalará y solucionará las posibles deficiencias del Reglamento de Protección de Datos, como ocurrió con la Directiva, dando pistas al legislador para reformas posteriores que resulten necesarias para proteger y garantizar a los titulares de datos un verdadero poder de disposición sobre su propia información , que es el objetivo último de este derecho"[130].

Definitivamente, en el marco de las redes sociales el ordenamiento jurídico no tiene establecidos mecanismos jurídicos suficientes y efectivos para poder solventar todos los riesgos que la introducción de datos personales a la Red pueden conllevar para la privacidad, ya que los sistemas actuales no permiten un control suficientemente efectivo, cuestión que se hace especialmente complicada cuando se trata de menores de edad. Los que están detrás de estas plataformas digitales deben de poner todos los medios necesarios disponibles para el establecimiento y efectivo control de sistemas de garantía y protección, sobre todo cuando se trata de menores, a pesar de los avances efectuados[131].
Es decir, además de una adecuada normativa a nivel internacional y nacional, que pueda adaptarse a la realidad de las redes sociales y a su constante cambio, también se necesita la colaboración de los propios proveedores de las plataformas, que deberán de contribuir a la seguridad de la privacidad.

En conclusión, el *big data* y las redes sociales como concreta manifestación, han supuesto un verdadero desafío para la protección de datos personales. Se han tomado una serie de medidas, como la modificación de la normativa europea de protección de datos, que han podido solventar ciertos problemas. Sin embargo, no es suficiente, debe existir una normativa con mayores capacidades de adaptación a los cambios constantes e inciertos de las tecnologías, ya que suponen nuevas amenazas en el tratamiento de nuestros datos pertenecientes a nuestra esfera más íntima. Además de la normativa, los entes que

[130] "El nuevo Reglamento de Protección de Datos Personales. Análisis de su eficacia en la determinación de su ámbito territorial y los remedios en caso de tratamiento ilícito" cit. 436
[131] "El fenómeno de las redes sociales y los cambios de vigencia de los derechos fundamentales" cit. 251

gestionan las plataformas digitales también deberán contar con mecanismos para proporcionar una mayor seguridad.
La protección de datos vive un momento decisivo, con retos constantes que obligan a escuchar atentamente las necesidades que se plantean (Agencia Española de Protección de Datos).

En mi opinión, considero que la sociedad no está concienciada de los peligros que supone exponer datos pertenecientes a su esfera personal en plataformas como las redes sociales, ya que éstas mismas no les proporcionan la suficiente información en el momento de suscribirse a éstas debido a que no les interesa ya que con esa cantidad masiva de datos, las plataformas digitales adquieren un poder extremadamente valioso.
Ya no solo es necesaria una especial atención a la normativa, tanto a nivel europeo como nacional, atendiendo a constantes modificaciones en consonancia con las innovaciones tecnológicas, sino que también debe impulsarse desde las instituciones públicas de los propios Estados una serie de advertencias sobre las consecuencias de dicho tratamiento y de los límites que tienen las empresas que gestionan el tratamiento de nuestros datos, ya que, a pesar de haber prestado nuestro consentimiento válidamente, no todo vale si ello supone la vulneración de derechos fundamentales como la protección de datos o la intimidad. Además, hay que aumentar las prerrogativas para pedir responsabilidad a los agentes que se dedican al tratamiento de datos, para así conseguir más garantías de protección de datos.

BIBLIOGRAFÍA

-AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS.

- Alarcón Caparrós, V., "GDPR: ¿qué necesitas saber del nuevo Reglamento Europeo de Protección de Datos? *Signaturit*, 2018 (disponible en https://blog.signaturit.com/es/las-claves-sobre-el-nuevo-reglamento-europeo-de-proteccion-de-datos).

-Carta de Derechos Fundamentales de la Unión Europea 2010/C 83/02 (Diario Oficial de la Unión Europea 30 de marzo de 2010).

-De Miguel Asensio, P. A., "Competencia y derecho aplicable en el Reglamento General de Protección de Datos de la Unión Europea" *Revista Española de Derecho Internacional,* vol. 69/1, 2017, Madrid, pp.75-108.

-Declaración Universal de Derechos Humanos, de 10 de diciembre de 1948.

-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 (BOE, 23 de noviembre de 1995).

-Durán Arroyo, A., "El nuevo Reglamento de Protección de Datos Personales. Análisis de su eficacia en la determinación de su ámbito territorial y los remedios en caso de tratamiento ilícito", *Revista Jurídica de la Universidad Autónoma de Madrid*, n.37, 2018, pp.415-440.

-Gil Antón, A. M., "El fenómeno de las redes sociales y los cambios de vigencia de los derechos fundamentales", *Revista de Derecho UNED,* n.10, 2012, pp. 209-255.

-Gil González, E., *Big data, privacidad y protección de datos*, BOLETIN OFICIAL DEL ESTADO, Madrid, 2016.

-Informe Jurídico de la Agencia Española de Protección de Datos 93/2008, sobre "Formas de obtener el consentimiento mediante Web. Conocimiento tácito."

-Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (BOE, 6 de diciembre de 2018).

- Pérez Luño, A. E., "*Derechos Humanos, Estado de Derecho y Constitución*", TECNOS, Madrid, 1986.

-Martínez de Pisón, J., "El derecho a la intimidad: de la configuración inicial a los últimos desarrollos en la jurisprudencia constitucional" *Universidad de la Rioja*, n.32, 2016, pp. 409-430.

-Minero Alejandre, G., "Presente y futuro de la protección de datos personales. Análisis normativo y jurisprudencial desde una perspectiva nacional y europea" *Anuario jurídico y económico escurialense,* n. 50, 2017, pp.13-58

- Recio Gayo, M., "*Big Data:* Hacia la protección de datos personales basada en una transparencia y responsabilidad aumentadas", *Revista de Derecho, Comunicaciones y Nuevas Tecnologías,* n.17, 2017, pp. 1-25

-Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS) (BOE 14 de mayo de 2016).

-Sentencia del Tribunal Constitucional de 30 de octubre 170/1987 (FJ 4).

-Sentencia del Tribunal Constitucional de 2 de diciembre 231/1988 (FJ 2).

-Sentencia del Tribunal Constitucional de 14 de febrero 21/1992 (FJ 3).

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

-Sentencia del Tribunal de Justicia de la Unión Europea C-131/12 de 13 de mayo de 2014, *Google Spain* (Diario Oficial de la Unión Europea, 7 de julio de 2014).

-Sentencia del Tribunal de Justicia de la Unión Europea C-230/14, de 1 de octubre de 2015, *Weltimmo* (Diario Oficial de la Unión Europea, 16 de noviembre de 2015).

-Sentencia del Tribunal de Justicia de la Unión Europea C-362/14, de 6 de octubre de 2015, *Schrems,* (Diario Oficial de la Unión Europea, 6 de octubre de 2015).

-Sentencia del Tribunal de Justicia de la Unión Europea C-191/15 de 28 de julio de 2016 (Diario Oficial de la Unión Europea, 26 de septiembre de 2016).

-Sentencia del Tribunal de Justicia de la Unión Europea C-518/07 de 9 de marzo de 2010 (Diario Oficial de la Unión Europea, 1 de mayo de 2010).

-Sentencia del Tribunal de Justicia de la Unión Europea C-362/14, de 6 de octubre de 2015.

-Suárez-Gonzalo, S., "Big Social Data: límites del modelo *notice and choice* para la protección de la privacidad" El profesional de la información, v.26, n.2, 2017 pp. 283-292.