Trabajo Fin de Grado

Análisis de los últimos avances normativos en materia de protección de datos. Especial referencia a las redes sociales (Instagram)

Presentado por:

María Fátima Broch González

Tutor/a:

José Díaz Lafuente

Grado en Derecho

Curso académico 2017/18

ÍNDICE

Abreviaturas

AEPD: Agencia Española de Protección de datos

AN: Audiencia Nacional

CDFUE: Carta de los Derechos fundamentales de la Unión Europea

CE: Constitución Española 1978

DPD: Delegados/as de protección de datos

GT29: Grupo de trabajo del artículo 29

LOPD: Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter personal

RGPD: Reglamento general de protección de datos

ST: Sentencia

TC: Tribunal Constitucional

TSJ: Tribunal Superior de Justicia.

UE: Unión Europea

I. INTRODUCCIÓN

La protección de datos de carácter personal es un derecho fundamental que plantea numerosos desafíos jurídicos a medida que su normativa va adaptándose a las necesidades del momento. Hace 10 años no existían los mismos conflictos en esta materia que los que tenemos hoy en día, pues la manera en la que nos comunicamos como personas ha cambiado totalmente, siendo función del Derecho armonizar esta realidad.

La finalidad de este trabajo es analizar las novedades normativas en relación con la protección de datos en el ámbito europeo y, por ende, en el ámbito nacional, con especial referencia a las redes sociales. Por este motivo, el trabajo se inicia en primer lugar, con un breve acercamiento a las redes sociales y a su impacto en la sociedad, para posteriormente abordar las fuentes jurídicas nacional y europea.

La elección de las redes sociales como caso práctico viene dada por la gran importancia creciente que tiene este instrumento novedoso en la sociedad y lo poco que realmente sabemos sobre a qué se destinan nuestros datos en estas plataformas, complicando aun más el desafío jurídico que ya existe en este ámbito. Supone un campo de especial aplicación del derecho, ya que aunque todavía poseen una corta vida, su desarrollo acelerado ha conseguido que la mayoría de las personas y empresas formen parte de estos espacios. Es decir, sin unas fronteras materialmente delimitadas lo que hace que, tal como señala MÓNICA ARENAS, “el reconocimiento del derecho a la protección de datos personales va de la mano de los avances científicos y tecnológicos experimentados, especialmente, en el terreno de la informática”[1].

Es una realidad social latente que conlleva una problemática jurídica relevante con respecto a la protección de datos[2]. Se transmite la idea de que la

[1] ARENAS, M. *Integración Europea y protección de datos personales. Las garantías especificas del derecho a la protección de datos personales.* Anuario de la Facultad de Derecho .Universidad de Alcalá, 2004-2005, vol. 2005, p.1 ISSN 1697-9699
[2] CHÉLIZ, MºC. *El “Derecho al olvido digital”.* Universidad de Zaragoza*,* 2016, p.262

protección de datos de carácter personal simboliza el reconocimiento de un derecho humano que se desarrolla por la evolución tecnológica[3].

En concreto, la red social elegida ha sido *Instagram* por ser considerada la red social del momento que, comprada por *Facebook*, se ha convertido en un espacio de vital importancia, por la vulnerabilidad tan grande que puede darse hacia la protección de datos. Al respecto he utilizado varias sentencias importantes para observar a qué nos referimos a la hora de interpretar la legislación cuando hablamos de datos de carácter personal o del control que pueden ejercer las personas titulares de este derecho y sentencias que contienen algunos casos mediáticos.

Para tratar adecuadamente la casuística que puede surgir, primero hemos de estudiar lacónicamente la normativa que se ha aplicado hasta el momento y así poder comprender y apreciar de forma adecuada las novedades que nacen en el seno de la Unión Europea y su importancia.

En primer lugar y a nivel nacional, tenemos el estudio de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal y el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de Desarrollo de esta ley. No encontraremos un extenso examen de la misma debido a que va a dejar de aplicarse, pero es importante ya que hasta que no se elabore una nueva ley nacional, esta será de aplicación con el límite de no transgredir las disposiciones que se encuentran en el RGPD.

A continuación, se encuentra una explicación detallada de las novedades que a este tema aporta, el Reglamento 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Este RGPD refleja un contenido adecuado a la manera en la que se han ido dando los diferentes problemas en la práctica y a la necesidad de adaptarse a los cambios tecnológicos y sociales. Es por ello un refuerzo necesario, más

[3] RICHTER, M. *Protección de datos de Carácter Personal como Derecho humano*. Revista Auctoritas Prudentium, Nº12, 2015. p.1

estricto y muy importante hacia la protección de datos[4]. Lo necesario es equilibrar los intereses socioeconómicos de las empresas y los derechos de los ciudadanos[5]. Al encontrarnos ante un espacio prácticamente nuevo, tanto desde el punto de vista de las novedades del RGPD como de las redes sociales, no existe numerosa interpretación de este campo al respecto.

A tenor de estas novedades, y al estar España adherida a la UE, nuestro país debe elaborar una ley orgánica nueva que se adapte a las directrices europeas, motivo por el cual, encontramos un examen del anteproyecto de ley en nuestro territorio nacional que va introduciendo algunas cuestiones al respecto.

Por último, destacaremos la política de privacidad de datos de Instagram en relación a todo lo anteriormente citado. De esta manera, podemos profundizar mejor en cuanto a cómo en la práctica se protegen los datos de los usuarios en una red social en concreto. La finalidad es observar si cumple todos los requisitos que exige el RGPD, haciendo una comparativa de la política de privacidad antes y después del RGPD y los problemas que se han ocasionado a razón de hacer un mal uso de los datos[6].

II. LAS REDES SOCIALES

1. ¿Qué son las redes sociales?

Para sumergirnos en el mundo de las redes sociales, primero hemos de definir su significado. Las redes sociales, según el subdirector del Laboratorio de Comunicaciones Multimedia ORIHUELA, son “espacios virtuales nuevos que nos permiten relacionarnos y donde construimos nuestra identidad dentro de un mismo punto de encuentro”[7]. Es decir, una red social es un espacio donde las personas que acceden a la misma se muestran con un perfil en el que

[4] FERNANDEZ, L. *El nuevo Reglamento Europeo de Protección de datos. Foro, Nueva época,* vol. 19, núm. 1, 2016. P.397
[5] BERROCAL, A. *Derecho de supresión de datos o derecho al olvido*. Madrid, 2017. p.9
[6] Caso Facebook y Cambridge Analytica.
[7] PÉREZ RUFÍ, J. *Estructura del mercado audiovisual: resultados*. Grupo de investigación Eumed.net ,Málaga, 2012, p.64

comparten sus gustos, opiniones y fotos interactuando con el resto de usuarios que, a su vez, comparten los mismos aspectos.

Como seres humanos, una de nuestras necesidades básicas es la comunicación y la podemos encontrar de muchas maneras. Las redes sociales se han convertido en un canal clave para hacerlo en nuestros tiempos. Para las personas que han nacido en la era de las tecnologías, las redes sociales, suponen un medio indispensable para acercarse a los demás, revolucionando así los antiguos métodos que han pasado a un segundo plano. Las redes sociales permiten conocer a personas diferentes y sus culturas, que de otra manera no habría sido posible o hubiera resultado muy complicado sin viajar continuamente o acercarse conscientemente al espacio físico de dichas personas para conocer su mundo.

2. La evolución de las redes sociales

El origen de las redes sociales comienza en 1995 con la creación de la web "classmates.com" por parte de su creador, Randy Conrads, quien la creó para poder encontrar antiguos compañeros y compañeras del instituto[8]. Tras el éxito y las posibilidades que ofrecía una plataforma de estas características, se le sumó en 2002 la red social *Friendster* con el mismo objetivo, pero creciendo a una velocidad importante, sumándose cada vez más usuarios que querían reencontrarse con sus antiguas amistades del colegio.

A partir de este momento, se empezaron a implantar redes sociales que hoy en día tienen un impacto grande en nuestra sociedad como *Facebook*, creada en 2004 la cual comenzó apoyando redes universitarias y terminó aceptando a cualquier usuario de Internet que no tuviera nada que ver con la finalidad original.

Actualmente existen varias redes sociales que son las más utilizadas por los usuarios, es decir, las más populares como son: *Twitter* (nacida en 2006),

[8] DÍAZ, A. Origen y evolución de las redes sociales Disponible en: http://socialmedialideres.com.ve/origen-y-evolucion-de-las-redes-sociales/

YouTube (lanzada en 2005) e *Instagram* (creada en 2010 y sobre la que versará el último punto de este trabajo). Al convertirse en las favoritas por los internautas, es aquí donde se concentrarán la mayoría de escenarios a regularizar por el Derecho.

Si observamos el punto de partida de las mismas, se crearon para dar forma a un deseo humano que es la comunicación, como ya hemos visto, pero han ido perfeccionando el "cómo" a medida que las personas han reflejado sus maneras de utilizarlas, en parte condicionadas por la clase de instrumentos que se les han proporcionado. Esto nos hace pensar que seguirán evolucionando. Un ejemplo claro es la presencia de las empresas en las redes sociales. Estas en un principio no estaban incluidas en la dinámica de la red, pero se han ido introduciendo de manera creciente, influyendo en los contenidos que ahora se encuentran en cualquier soporte digital. Por ejemplo, la publicidad común de sus productos o publicidad a través de personas con un gran número de seguidores, a quienes regalan sus artículos.

3. Impacto de las redes sociales en la ciudadanía

A medida que como sociedad vamos evolucionando, la manera en la que nos comunicamos, en que guardamos nuestros datos, los soportes que utilizamos y la protección que elegimos, estos también lo hacen. La mensajería mediante cartas ha sido sustituida por plataformas como *WhatsApp*, situación que ha derivado en la modificación de nuestra manera de concebir la comunicación creándose, como hemos explicado, múltiples "redes sociales" que atienden a las nuevas necesidades sociales.

En su día, STANDLEY MILGRAM, psicólogo social que dedicó muchos años de su carrera a demostrar el comportamiento humano mediante experimentos, quiso poner a prueba la hipótesis de que todos los seres humanos estábamos interconectados y que podíamos contactar con cualquier otra persona en 6 movimientos.

Su experimento dio por válida la hipótesis, a la que llamó “el problema del pequeño mundo”[9]. Esta idea es la que hace que las redes sociales triunfen, aunque si bien es cierto que el experimento probó la idea para comunidades cerradas y no para una red infinita como Internet, sí que explica muchos puntos importantes, como que los comportamientos de los individuos en las redes sociales se contagian[10]. Esto podría explicar que en una red social, las personas que observan determinadas tendencias, copien las mismas y se cree un sentimiento de pertenecer a la consciencia colectiva.

Desde el punto de vista del Derecho, una red social se convierte en un escenario importante donde las personas actúan y se relacionan, creándose múltiples cuestiones jurídicamente complejas. Al ser un campo nuevo de situaciones, el Derecho debe adaptarse a los diferentes escenarios, delimitando las leyes relativas a la seguridad, la libertad de expresión, el flujo correcto de los datos, la intimidad, la privacidad, etc. España, al ser un país integrante de la Unión Europea, debe para ello poner la mirada en el Reglamento UE 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 en relación con la LOPD y el cual analizaremos con respecto a estos temas.

El problema de la desinformación por sobreinformación o la “hiperaccesibilidad” también debe ser un tema abordado por la legislación[11]. Para transmitir un mensaje se necesita un canal, en este caso, el canal es la red social y si millones de personas tienen a su alcance este instrumento para publicar ideas, afirmaciones, estudios, etc., existe el riesgo de que nadie contraste dicha información y todo el mundo pueda crear una idea falsa que transmite al resto. Esto supone un mal uso de la red social[12].

---

[9] WATTS, D. *Seis grados de separación, la ciencia de las redes en la era del acceso*. Barcelona, 2006. p.39

[10] NOAIN, A. La protección de la intimidad y la vida privada en internet*: La integridad contextual y los flujos de información en las redes sociales.* Agencia Española de Protección de Datos, Madrid, 2015. p.168

[11] SIMÓN, P. *El reconocimiento del derecho al olvido digital en España y el la UE*. Barcelona 2015. p.61 y 67

[12] BRAVO, A. *Utilidad y perjuicio en la red social*. Disponible en: http://www.revista-critica.com/la-revista/monografico/24-primeras-personas/37-utilidad-y-perjuicio-en-la-red-social

Existen numerosas redes sociales en las que una misma persona puede interactuar. Cada una de esas redes no contempla unas fronteras de países porque dentro de ellas puede haber personas de numerosos lugares, opiniones, culturas y maneras de entender el mundo completamente diferente. Esto es equiparable a que, de forma física, personas de todo el mundo con pluralidad de ideas, se relacionen entre sí en un mismo espacio físico en el que comparten sus experiencias. Algunas estarán de acuerdo en cuanto a gustos, aunque no compartan el mismo idioma, y otras aún hablando la misma lengua, pueden estar en desacuerdo por discernir sobre un tema polémico.

Toda la información que los usuarios comparten en las redes, es material que no se puede procesar de manera tradicional, por lo que forma parte del *Big Data*. Nos referimos a este concepto cuando hablamos de la administración de grandes flujos de información y que suponen un valor importante para las empresas, ya que pueden estudiar los patrones que se repiten en los consumidores ante variables dependientes y así ofrecerles ideas más adaptadas a sus gustos[13]. Es importante porque el 98% de la información que existe hoy en día está digitalizada. El *Big Data* analiza ficheros de datos, por lo que este flujo de datos ha de regularse legalmente.

Dado que las redes sociales son una de las entidades que más utilizan hoy en día los beneficios del *Big Data*, existen cuestiones que deben delimitarse porque al fin y al cabo lo que se recoge y se transforma son datos, datos que muchas veces son de carácter personal expresados de muchas formas como "*likes*" o preferencias sobre unos gustos u otros, pero que siguen siendo datos. El Tribunal Constitucional en la sentencia 94/1998 de 4 de mayo recoge que se trata de un derecho fundamental a la protección de datos orientado a garantizar por ello, el control de la persona sobre sus datos y es algo que se escapa del ámbito del *Big Data*, ya que la mayoría de las personas no saben a qué exactamente se destinan los mismos[14].

[13] GIL, E. Big Data*, privacidad y protección de datos.* Agencia española de protección de datos Madrid, 2016, p.28.
[14] BERROCAL, A. *Op.cit* p.10

Además, el artículo 10 de la CE señala que estamos ante un derecho que se manifiesta en el derecho de la dignidad de la persona y al libre desarrollo de la personalidad, de manera que todas estas cuestiones que giran en torno a Internet, afectan muchísimo más de lo que pensamos a la ciudadanía.

Recientemente, y como veremos más adelante, encontramos el caso mediático de *Facebook y Cambridge Analytica*, en el cual se observa este problema reflejado: datos de usuarios empleados sin consentimiento lícito, con otros fines ajenos a los de la propia red social.

4. Redes sociales y menores

Desde que han empezado a emerger estos modelos de comunicación, es muy frecuente que niñas y niños tengan en su poder dispositivos móviles con los que se puede acceder a las redes sociales. A la hora de crearse un perfil, los menores solo necesitan poner una fecha de nacimiento inventada para acceder, fecha que nadie va a contrastar o verificar, por lo que el acceso resulta muy fácil.

Una vez creado el perfil, es complicado establecer un control absoluto sobre los contenidos a los que los menores acceden, sobre todo en el consentimiento que prestan a la hora de aceptar los términos de privacidad dentro de cualquier aplicación[15].

Como este control es difícil, supone un problema el hecho de proteger los datos de los menores en las redes sociales[16]. Dada la novedad, hay muchas cuestiones que aún no se han regulado completamente, suponiendo nuevos retos para todas las personas entendidas del derecho como juristas, jueces, legisladores y el Ministerio fiscal, quien dentro de sus funciones se encuentra la de velar por el bienestar de los menores.

[15] BARRUISO, C. *Anuario de la Facultad de Derecho.* Universidad de Alcalá*,* 2009, no.2 ISSN 1888-3214, p. 313.
[16] TRONCOSO, A. *Las redes sociales a la luz de la propuesta de reglamento general de protección de datos personales*. Revista Derecho, parte II, Universidad Oberta de Catalunya. p.37

Debería implantarse un mecanismo de verificación entre el nombre y los apellidos de la persona, así como su fecha de nacimiento, o bien incluir un apartado eficaz donde quede constancia fehaciente de que el padre o el tutor del menor está de acuerdo con que el mismo interactúe en un espacio virtual. Se hace necesario ya que el menor que entra en una red social sin el consentimiento de sus padres lo hace a tiempo real y esto dificulta aún más el control que debería ser continuo.

Esto sirve de premisa para muchos delincuentes que ponen la mirada sobre los menores, a los que se les facilita el camino por tener contacto con los mismos sin ninguna vigilancia. Muchos se aprovechan de situaciones en las que existe un conflicto de convivencia entre padres e hijos, ganándose la confianza del menor para que más adelante se vean físicamente, vendiéndoles mientras tanto una idea o identidad falsa. El problema se incrementa cada día más al juntar estos factores: la inocencia del menor, la ignorancia de los padres ante este tema y el aprovechamiento de los dos anteriores por personas que tienen la intención de cometer una acción ilícita.

En el siguiente punto analizaremos algunas cuestiones y soluciones relativas a este tema de los menores en las redes sociales que ha abordado, por ejemplo, el TC interpretando la ley.

III. ANÁLISIS DE LA NORMATIVA NACIONAL Y EUROPEA EN RELACIÓN CON LA PROTECCIÓN DE DATOS

1. Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal

En el marco nacional de España, la protección de datos de carácter personal está regulada por esta LOPD. Esta Ley es el resultado de la trasposición de 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 los mismos.

Es una Ley Orgánica, ya que como su artículo 1 indica, garantiza en materia de tratamientos de los datos personales, los derechos fundamentales de las personas físicas, y todos los derechos fundamentales, deben ser desarrollados por leyes orgánicas en base al artículo 81 CE. Este derecho fundamental se recogió también en el artículo 8 de la CDFUE.

Analizados el ámbito de aplicación de esta ley, artículo 2 de la LOPD, observamos que las redes sociales no se encuentran enumeradas en los ámbitos excluidos. Es aplicable la legislación nacional, cuando el tratamiento de los datos se lleva a cabo en el territorio nacional dentro de las actividades propias de un establecimiento del que esté al mando el responsable del tratamiento de datos. También cuando el responsable de los datos no se encuentra en el territorio nacional pero le es aplicable la legislación por cuestiones de Derecho Internacional Público. Por último, cuando el responsable del tratamiento no se encuentre en la Unión Europea, pero en el tratamiento de los datos utiliza medios que se encuentran en España. Estamos frente a un ámbito de aplicación que en principio parece amplio, pero que como el propio artículo indica, se supedita a que las actividades del responsable se encuentren en el territorio nacional entre otras.

En este sentido, debemos matizar la cuestión de que no son de aplicación, como dice el artículo 2.2, los ficheros en el ejercicio de actividades únicamente personales o domésticas. Conviene delimitar cuáles son, por tanto, estas actividades de carácter personal o doméstico.
Acudimos para ello a la ST de la AN del 15 de junio 2006 donde se señala que: “Será personal cuando los datos tratados afecten a la esfera más íntima de la persona, a sus relaciones familiares y de amistad y que la finalidad del tratamiento no sea otra que surtir efectos en estos ámbitos”.

Un informe emitido por la AEPD recoge una consulta en la que se discute si en relación a la LOPD, una red social deportiva puede publicar materiales audiovisuales donde aparecen menores quienes previamente habían subido a

la red *YouTube* material que luego era enlazado con *Facebook*, por medio de esta red social deportiva. En principio parece que no es de aplicación ya que no se supera el carácter "personal", pero la realidad es que en numerosas ocasiones sí se supera esta barrera, por no existir un límite para su acceso[17].

La Sentencia de 6 de noviembre de 2003 TSJ de las Comunidades Europeas explica que se extralimita el ámbito privado si el tratamiento de los datos tiene como fin la divulgación de los mismos y sean accesibles a un sin fin de usuarios, imposibles de contabilizar.

En relación con la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995 se crea un grupo de trabajo sobre la protección de las personas en lo que respecta al tratamiento de datos personales. Emitieron el Dictamen 5/2009 sobre redes sociales en línea, adoptado el 12 de junio de 2009, en el que en su punto 3.1.1, referente al *Objeto y naturaleza*, se encarga de especificar que, aunque los datos a los que un usuario puede acceder están reducidos a los contactos de su elección, hay usuarios con un número muy alto de contactos y esto precisa que no sea de aplicación el apunte de "actividad exclusivamente personal o doméstico*".*

Viene a explicar cómo se debe entender la definición que proporciona la LOPD respecto a esta actividad de carácter personal o doméstico que no está dentro de los ámbitos de aplicación de la ley, y que se supera cuando el número de personas invitadas a ver a los datos es alta o no existe un filtro para que accedan al contenido[18]. Sin estas aproximaciones sería difícil determinar cuando estamos ante el ámbito meramente doméstico y cuando nos encontramos en el límite.

En el artículo 3 de la LOPD se recoge una lista de definiciones para comprender los conceptos a los que la ley se refiere. Un concepto clave es el de "*Interesado*" que, en virtud de este artículo, podemos afirmar que se trata de la persona titular de los datos que van a ser objeto de tratamiento, figura que inspira esta ley Orgánica.

También acudimos al mismo para entender qué es un dato de carácter personal: "Datos de carácter personal: cualquier información concerniente a

[17] Agencia Española de protección de datos, *Informe 0197/2013,* p.5

[18] RALLO, A. *Protección de datos personales y redes sociales: obligaciones para los medios de comunicación*, Quaderns del cac, 2014, p. 44.

personas físicas identificadas o identificables". Una persona empieza a ser identificable cuando se puede fijar su identidad por información sobre la misma, como información social, cultural, pensamientos, *hobbies*, etc.

El TC se pronunció acerca de este aspecto manifestando que también están protegidos los datos que aunque no sean de la vida privada, sirvan para identificar a la misma por servir para poder crear un perfil ideológico o económico de la persona con los datos que publica[19]. Dentro de los datos de carácter personal también se encuentran los "*likes*" en las fotos que se comparten, ya que con ello se deja constancia de las preferencias que la persona tiene acerca de gustos o ciertas publicaciones frente a otras[20].

El anteriormente citado Grupo de trabajo del artículo 29 sobre protección de datos emitió otro Dictamen, el 4/2004, esta vez relativo al tratamiento de datos personales mediante vigilancia por videocámara, del que se ha servido la AEPD concluyendo que "los datos constituidos por imagen y sonido son personales", y lo son porque mediante los mismos la persona se puede identificar.

En relación a las redes sociales, si las imágenes captadas en una cámara de videovigilancia se utilizan para publicarse en *YouTube* o al efecto en *Facebook*, plataformas a las que cualquier usuario puede acceder, y a tenor del artículo 6.1 de la LOPD, estas imágenes están limitadas al consentimiento que presten las personas que aparecen en las mismas[21].

En el Título II de esta ley encontramos los principios referentes a la protección de datos, como la calidad de éstos, el derecho de información en la recogida de datos, el consentimiento del afectado, los datos especialmente protegidos, los datos relativos a la salud, la seguridad de los datos, el deber de secreto y la comunicación de datos. El tratamiento de los datos que se encuentra en las redes sociales debe cumplir con estos principios. Son una transposición de la Directiva Europea 95/46/CE, esto es, emanan de la misma, pero en este sentido la LOPD es más estricta.

---

[19] NOAIN, A. *Op.cit*. p.168.
[20] GIL, E. *Op.cit.* p. 45
[21] RALLO, A. *Op.cit*. p. 44.

Un punto muy importante a estudiar es el relativo al consentimiento. El consentimiento que los usuarios prestan en las redes sociales tiene que ser un consentimiento previamente informado, tal como recoge el artículo 5.1 LOPD, que significa que el usuario debe conocer, antes de "aceptar", la finalidad y el tratamiento que van a tener sus datos , prestando así un consentimiento válido y consciente.

La manera en la que el interesado recibe esa información ha de ser clara, expresa e inequívoca, ya que si fuera de otra forma el resultado podría no ser el mismo, es decir, si la información en relación al consentimiento que un interesado recibe en una red social no es clara e inequívoca, su consentimiento no estará suficientemente informado. Como podemos observar en la ST del TS 3257/2018, sala de lo contencioso, lo único que exime de prestar el consentimiento del interesado hacia sus datos es si viene establecido por la ley, haciendo alusión al artículo 11 de la LOPD.

Debe prestarse de manera inequívoca para que sea posible el tratamiento de los datos, así lo recoge también el artículo 6 de la LOPD en su apartado 1. Cuando una persona se crea un perfil en cualquier red social, como por ejemplo en *Instagram*, debe aceptar una política de privacidad y tratamiento de datos con lo que, si termina aceptando, accede a prestar su consentimiento al tratamiento de sus datos. Realmente este consentimiento informado en la práctica no es proporcionado de manera eficaz por el usuario, por presentarse dicha política de manera extensa, densa, rígida y poco dinámica.

No es lo mismo recibir en mano un papel detallado con los objetivos claves del tratamiento de datos de forma clara que tendría una lectura rápida, que un documento digitalizado y demasiado extenso. Es decir, los escenarios que nacen del *Big Data* hacen que no se preste un consentimiento válido, tal como se precisa en la LOPD: consentimiento expreso, libre, inequívoco e informado[22].

[22] GIL, E. *Op.cit.* p. 61-66

Existe un baremo de edad en *Instagram* que verifica cuaáles son los usuarios que más utilizan la red social y qué edad tienen, siendo de 16 a 24 años. Es lógico pensar que la mayoría de la gente va a aceptar los términos proporcionados por la red social en cuanto al tratamiento de sus datos, porque no ofrece tampoco una alternativa de aceptar parcialmente algunas condiciones[23]. Un ejemplo claro es la condición de recibir publicidad en su muro, cuestión que el usuario debe consentir sin alternativa para acceder a la red social, esto pone en entredicho el significado real de "consentimiento libre".

Las redes sociales son mundialmente conocidas por su labor de distracción, lo cual supone que una persona cuando accede en una de ellas lo hace para distraerse de la rutina, relacionarse con los demás, despejarse durante 5 minutos poniéndose al día del contenido que han subido sus contactos. Esto crea una idea de comunidad, de bienestar, que en la mayoría de los casos poco se relaciona con el peligro de compartir datos sin saber qué tratamiento real reciben[24].

Es esta falta de conexión entre el peligro y la ignorancia del destino de los mismos lo que hace aún menos atractiva la idea de leer un documento con palabras demasiado técnicas y que requiere emplear un tiempo considerable. Se utiliza la necesidad de comunicarse, base del éxito de las redes sociales, con la premisa de la gratuidad económica que tiene mucha menos importancia que el real trasfondo de un derecho fundamental que consentimos, sin saberlo, que se vulnere[25]. Realmente cabe preguntarse qué mueve a la sociedad para "regalar sus datos" de forma tan gratuita, sometidos a un control empresarial o analítico evidente del que nadie es consciente[26].

---

[23] PERIODICO DE NOTICIAS El país. *Mar España: "Seremos beligerantes con todas las redes sociales*". 24 Mayo 2018. Disponible en: https://elpais.com/economia/2018/05/22/actualidad/1527003631_400767.html

[24] BARRUISO, C. *Op.cit* p.321

[25] ESCRIBANO, P*. Los derechos a la intimidad y a la privacidad en el siglo XXI*. Madrid 2015. p.72

[26] ARENAS, M. *El valor de la información personal: protección de datos personales y la sociedad del espectáculo*. Anuario de la Facultad de Derecho. Universidad de Alcalá, 2009, no.2. p.295. ISSN 1888-3214

La Audiencia Nacional invocó el artículo 6 LOPD en una sentencia de 2 de enero de 2013 posicionándose a cerca del consentimiento. Un usuario de la red social *Facebook*, había publicado un vídeo en su muro donde aparecían menores de edad de 7 y 8 años. El problema que se plantea en una red como esta, donde la mayoría no tienen un acceso al perfil restringido, es que se extralimita el ámbito personal o doméstico al que ya nos hemos referido porque cualquier usuario puede acceder a esta información. La cara de los niños era perfectamente reconocible, por lo que estamos dentro de lo que se considera "*dato de carácter personal*". Los padres de los menores no habían prestado el consentimiento para tal fin, por lo que la Audiencia Nacional declaró que había una infracción por vulneración del principio de consentimiento[27].

El consentimiento que han de prestar los padres o los tutores de los menores debe entenderse por un lado desde la obtención de la fotografía o material de video y por otro lado a la publicación en la página web o red social, ya que esto supone una cesión o comunicación de datos de carácter personal tal y como recoge el artículo 3.J LOPD: "Toda revelación de datos realizada a una persona distinta del interesado" [28].

Esta ley, por tanto, confiere una protección de los datos de carácter personal de la que es consecuencia una responsabilidad. Responsabilidad por un lado del responsable de tratar los datos, conforme al artículo 9 de la LOPD, utilizando medios para que se evite su alteración, pérdida y tratamiento no autorizado como ante terceros que no nos hayan prestado su consentimiento para que publiquemos contenidos donde se les pueda identificar como fotos, videos, audios con su voz, entre otros.

Así la Ley Orgánica 1/1982 referente a la protección civil del derecho al honor, la intimidad personal y familiar y a la propia imagen, de 5 de mayo, ha de ponerse en relación con la LOPD, ya que si lo hacemos podemos infringir estos derechos de intimidad personal y demás.

[27] Agencia Española de protección de datos, *Informe 0197/2013,* p.1
[28] RALLO, A. *Op.cit.* p. 44.

En este sentido, hay que estudiar la actuación que puede llevar a cabo un medio de comunicación en una red social, pues debe tener en cuenta todo los que hemos visto hasta ahora para cumplir con la LOPD. En este sentido, el profesor ARTEMI RALLO, Catedrático de Derecho Constitucional de la Universidad Jaume I, recoge una serie de recomendaciones a seguir por los medios de comunicación que quieran abrirse un perfil en *Facebook* para que estén en armonía con la LOPD.

En primer lugar, que cumplan con el deber de información al que ya hemos hecho alusión porque los datos que se utilicen y su tratamiento, deberán cumplir con lo establecido en el artículo 5 de la LOPD.

En este sentido la recomendación que se hace es presentar la información de manera resumida o breve, en la cuenta que la red social facilita con acceso a la información relevante al responsable, también al objetivo que se busca y las formas de ejercicio de los derechos. Además, destaca otras recomendaciones como: poner a disposición un mecanismo que permita enviar un mensaje con esta información a nuevos amigos, informar en particular si el tratamiento de los datos va a tener un fin comercial directo, o el tratamiento de datos sensibles.

Por otro lado, y en la línea de lo que ya hemos señalado, la siguiente recomendación va dirigida al consentimiento, que señala como causa legítima del tratamiento de los datos personales, en relación al artículo 6 LOPD. Para este punto la recomendación prestada es aclarativa sobre cómo debe ser este consentimiento que solo afecta a la persona que se agrega. Señala también que las posibles excepciones en cuanto al consentimiento deben estudiarse en el caso concreto con las circunstancias del mismo.

También se recoge el recordatorio de que un perfil abierto no supone la existencia de consentimiento. Deben regir los derechos de rectificación, cancelación y oposición al tratamiento. En este sentido cabe hacer un paréntesis y acudir al artículo 5.d de la LOPD en relación al artículo 16 de la misma ley. El artículo 5, en su apartado “d”, especifica que en la información

que se da a los interesados debe ir incluida la posibilidad para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

El artículo 16, por su parte, desarrolla dichos derechos responsabilizando al responsable del tratamiento, en este caso la red social, a que estos derechos se hagan efectivos con un plazo máximo de 10 días. Volviendo a la recomendación del profesor ARTEMI RALLO, este derecho de rectificación podemos traducirlo en el mundo virtual como el derecho de un usuario a poder elegir sobre la eliminación de un comentario suyo en un determinado muro o desistir en la relación iniciada con un usuario "dejar de seguir a esa persona[29]". Es decir, que la información que un usuario emite en una red social como un "Me gusta", una foto, un comentario, una opinión pueda ser rectificada, no enviada de manera permanente porque la persona tiene derecho a cambiar de opinión sobre las distintas acciones que se pueden llevar a cabo en una red social.

Por último, como colofón a las recomendaciones, se incluye aquella que ha de regir los principios de seguridad y secreto que deberán adaptarse al entorno concreto. En este sentido, los principios de seguridad y secreto los encontramos recogidos en los artículos 9 y 10 de la LOPD. De esta seguridad se encarga el responsable del fichero, es decir, la red social en cuestión que debe asegurar los datos de la manera que ya se ha apuntado y, además, guardar el deber de secreto de modo que mientras se traten los datos el responsable esté obligado al secreto profesional.

Si una red social al uso, en todo lo relativo a los deberes que debe cumplir y por los que es responsable (tal y como señala el artículo 3 LOPD d) "Responsable del fichero o tratamiento: persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento."), no cumple con los mismos, la persona cuyos datos se han visto utilizados con distinto fin al que ha consentido o sufra daños o lesiones en sus derechos tiene derecho a una indemnización. Lo

[29] RALLO, A. *Op.cit.* p.46

encontramos en el artículo 19 de la LOPD. Es una garantía para los interesados que vean perjudicados sus bienes o derechos por el incumplimiento de los deberes que recoge la ley y que debe llevarse a cabo por los responsables. Es un límite a la actuación de los responsables, proporcionando a los interesados un instrumento de defensa de sus derechos. Encontramos ficheros de titularidad pública o ficheros de titularidad privada, en nuestro caso son ficheros de titularidad privada que se rigen entonces por órganos de jurisdicción ordinaria.

2. Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de Desarrollo de la Ley 15/1999

Un Real Decreto es la decisión aprobada por el Consejo de Ministros y firmada por el Rey, que viene a aprobar un Reglamento que desarrolla una Ley[30]. En este caso, el Real Decreto 17/2007 aprueba el Reglamento que desarrolla la LOPD derogando, además, el Real Decreto 994/1999 de medidas de seguridad de los ficheros automatizados que contengan datos personales.

Existe un cambio de perspectiva muy importante, debido a que, a diferencia del anterior Real Decreto, este empieza a considerar la materia relativa a la seguridad tanto el tratamiento automatizado de los datos de carácter personal, como el no automatizado, adaptándose a las nuevas exigencias de la sociedad y fijando criterios de aplicación a ambos tipos. Una red social se configura en un espacio virtual, por lo que el tratamiento de los datos que se susciten dentro de la misma será automatizado. Pero la novedad del tratamiento a ficheros no automatizados se da para proteger, por ejemplo, historiales médicos en papel, datos que no tengan está protección por no estar controlados; pero deben estarlo porque hoy en día hasta un marcapasos es *hackeable*[31].

---

[30] MUÑÓZ BARRIOS, A. *Tipos de decretos en España: Real Decreto, Real Decreto Legislativo y Real Decreto Ley.* Disponible en: http://queaprendemoshoy.com/tipos-de-decretos-en-espana-real-decreto-real-decreto-legislativo-y-real-decreto-ley/

[31] PERIODICO DE NOTICIAS EL MUNDO. *Los marcapasos se pueden hackear*. 29 Mayo 2017. Disponible en: http://www.elmundo.es/tecnologia/2017/05/29/592be6a7268e3ecf4e8b4642.html

Además, la Ley 24/2002, de 11 de junio, de Servicios de la sociedad de la información y comercio electrónico, junto con la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, facultan a la AEPD en materia sancionadora, y dichas leyes precisan de un desarrollo Reglamentario que se encuentra en este Reglamento 17/2007. La finalidad es desarrollar los procedimientos que tiene que llevar a cabo la AEPD en tanto en cuanto tiene potestad sancionadora, pero necesita de la previa reclamación al responsable o la responsable del tratamiento para acudir a la misma[32].

Como no podía ser de otra forma, tanto la LOPD como este Reglamento, comparten el mismo objetivo: regular los distintos riegos que pueden suscitarse en el marco del tratamiento de datos ante los derechos de la personalidad. En la LOPD encontramos las líneas generales que ahora van a ser desarrolladas por el Reglamento, tanto en relación a los principios de la Directiva, como en las necesidades que han ido surgiendo en cuanto a la interpretación de la LOPD.

La estructura del Reglamento se divide en 9 Títulos. El Título I explica cuál es el objeto y ámbito de aplicación que, como hemos dicho, es el desarrollo de la LOPD y las disposiciones relativas a la potestad sancionadora de la AEPD. Así se recoge en el artículo 1.

También centra el ámbito territorial de aplicación del Reglamento en su artículo 3, especificando que será aplicable en la misma medida que ya enuncia la LOPD, no aportando ninguna aproximación que clarifique cuestiones al mismo ámbito.

Dentro de este primer título, se desarrolla la idea recogida en el artículo 2.2 LOPD, dada la necesidad de explicar de forma exhaustiva lo que se entiende por ficheros y tratamientos relacionados con actividades personales o domésticas. Se trata de una cuestión muy importante ya que estos ficheros están excluidos de la aplicación de la LOPD y, por lo tanto, de este Reglamento.

[32] *9a Sesión Anual Abierta de la AEPD. Centro de Conferencias Fundación Pablo*

Así, en el artículo 4 del Reglamento se especifica que solo se considerarán relacionados con actividades personales o domésticas los tratamientos relativos a las actividades que tienen lugar en la vida privada o familiar de las personas. Pero conviene recordar, que sí se extralimita este ámbito cuando en una red social el contenido no tiene un filtro para limitar el número de visitas como ya observamos.

En la LOPD, el artículo 3 es el encargado de recoger las definiciones de conceptos relativos a este tema. El reglamento introduce nuevos conceptos para comprender mejor los ya recogidos en la LOPD. Resulta necesario por el lenguaje tan técnico, tal como figura en el artículo 5. Se incluye una definición nueva como es la de “Fichero no automatizado” y se explica que se trata de todo conjunto de datos de carácter personal que se organizan de una manera no automatizada, permitiendo acceder a datos de carácter personal sin esfuerzos desproporcionados. Por lo que entonces, un fichero automatizado es una red social, porque se configura como una base de datos que no se encuentra en formato papel.

Se introduce, a modo aclaratorio también, el apartado “o” de este artículo 5, para saber a qué nos referimos cuando hablamos de persona identificable. En el artículo 3 LOPD, se observa que por datos de carácter personal se entienden todos aquellos que identifican a una persona, idea que ya teníamos delimitada. Se señala que las personas son identificables cuando su identidad pueda determinarse de manera directa o indirecta, por cualquier información sobre su fisiología, su economía. Este detalle deja claro aún más claro que todos los datos que se manejan en una red social tienen la consideración de datos de “carácter personal”, sobre todo, porque todo lo que podemos encontrar en la misma son datos que identifican al usuario.

Este artículo 5 en su apartado “Q”, aporta una definición más amplia de lo que se entiende por un “Responsable”. Si lo aplicamos a una empresa que se incluye en las redes sociales, hay que considerar lo siguiente: un responsable, como hemos dicho, es el encargado de dar tratamiento a los datos de carácter

personal, pero en una red social, el responsable (empresa) es a la vez también usuario de la misma.
Por tanto, sobre el tratamiento que se da, la empresa no tiene control, por ejemplo, sobre el fichero de la red. Las obligaciones entonces son distintas, no será necesario que se inscriba un fichero ni que se formalice un contrato de acceso a datos por cuenta de terceros, sino que más bien, la empresa debe adaptarse a las herramientas que la propia red social ofrece y que muchas veces se trata de una autorregulación[33].

El profesor ARTEMI RALLO, explica que para que se pueda afirmar que se actúa como una persona usuaria más han de darse las condiciones de que se comporte como una persona jurídica que interactúa en la red, que no se incorporen datos personales a recursos propios o no pactar servicios adicionales como emisión de publicidad[34].

Lo más importante del Título II del Reglamento es que, dentro de los principios de la protección de datos, se centra fundamentalmente en la regulación de la forma de obtención del consentimiento, sobre todo, ante servicios de comunicaciones electrónicas como pueden ser las redes sociales y la captación de los datos de los menores.

El artículo 12 explica que la solicitud que se presenta para que la persona proporcione su consentimiento, debe ir relacionada con una serie de tratamientos concretos y dejando bien claro cuál será la finalidad de los mismos. Una vez más, se habla de la importancia de que ese consentimiento esté previamente informado, de manera que se conozca inequívocamente la finalidad de los datos. Se añade que será el responsable quien tenga la carga sobre la prueba de que ha existido un consentimiento válido y que puede hacerlo mediante cualquier prueba admitida en derecho. En las redes sociales,

[33] Revista de prensa, *AEPD publica un sistema de notificación electrónica para comunicar la designación de Delegados de protección de datos*. Disponible en: https://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2018/notas_prensa/news/2018_04_10-ides-idphp.php
[34] RALLO, A. *Op.cit.* p. 46

es preciso prestar nuestro consentimiento para poder acceder a las mismas, como ya hemos explicado.

En el siguiente artículo 13, se desarrolla el consentimiento para tratar los datos de los menores. Se distingue entre los menores de 14 años y los que aún no hayan alcanzado dicha edad. Se permite que los mayores de 14 años presten su consentimiento para el tratamiento de sus datos de carácter personal, siempre y cuando una ley no exija para su prestación que sean asistidos por sus padres o tutores legales. Por debajo de los 14 años, se especifica que será necesario para el tratamiento el consentimiento de los padres o tutores legales del menor.

Se expresa que la manera de dar la información a los menores para que presenten su consentimiento tiene que ser mediante un lenguaje fácilmente comprensible por ellos, verificándose por parte del responsable del tratamiento la edad del menor y la validez de su consentimiento prestado, así como en su caso, el de sus padres o tutores. En el artículo 14, encontramos cómo es necesario que se ponga a disposición del interesado un medio sencillo y de carácter gratuito para recoger la negativa al tratamiento de sus datos de carácter personal y a su finalidad.

En cuanto al Título III, que se refiere a los derechos de acceso, rectificación y oposición y a diferencia de la LOPD, se recoge aquí el carácter personalísimo de los mismos, en el artículo 23. En la LOPD, estos se encuentran regulados en los artículos 15 a 17, pero no especifica que tengan carácter personalísimo, que significa que solo pueden ser invocados por el interesado.

En este sentido, cabe destacar la Instrucción 1/1998, de 19 de enero, de la AEPD, relativa al ejercicio de los derechos de acceso, rectificación y cancelación. En su Norma Primera se señala que estos derechos son personalísimos y deben ser ejercidos por el afectado ante el responsable del fichero, para lo que se hace necesario, lógicamente, que la persona interesada o afectada verifique su identidad. Una vez comprobada su identidad, éste pedirá una solicitud para ejercer estos derechos.

El TC, en su Sentencia nº 292/2000, expresa que estos derechos forman parte de las facultades que provienen del derecho fundamental a la protección de datos y cito textualmente “sirven a la capital función que desempeña este derecho fundamental: garantizar a la persona un poder de control sobre sus datos personales, lo que solo es posible y efectivo imponiendo a un tercero los mencionados deberes de hacer”.

El artículo 34.C del Reglamento recoge la especialidad de que el derecho a la oposición puede hacerse si el tratamiento es únicamente automatizado, por lo que en una red social podemos ejercer este derecho porque el tratamiento no tiene lugar en formato papel.

Un aspecto esencial de este Reglamento se encuentra en el Título VIII, el relativo a la seguridad que deben emplear todas las organizaciones que traten datos personales. El Reglamento en este sentido, contiene una importante consideración a los niveles de seguridad que se pueden dar en los distintos casos.
El nivel básico se reserva para cualquier tipo de fichero, por lo que las redes sociales deben incluir este nivel para poder funcionar conforme a derecho, artículo 81 del Reglamento. En el apartado 2.F se indica que si los datos permiten ver aspectos de la personalidad o comportamiento de la persona, el nivel será medio.

En este sentido, y trayendo a colación que el *Big Data* tiene un valor preciado para las empresas por poder estudiar los comportamientos de las personas y sus preferencias mediante, por ejemplo, las publicaciones que más se visitan en una red social se determina que en las redes sociales debe existir un nivel medio de seguridad en virtud de este artículo 81.2.F puesto que constantemente se estudian los patrones de comportamiento no solo de una persona, sino de todas.

3. Reglamento 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril, 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

Aunque su fecha data del 25 de mayo de 2016, empezó a desplegar sus efectos el 25 de mayo del presente año 2018. El motivo radica en ofrecer a los Estados Miembros un plazo de adaptación de este Reglamento a la nacional. Con la aplicación del Reglamento, deja de estar en vigor la LOPD 15/1999 y la Directiva 95/46/EC.

El Reglamento europeo incluye 173 consideraciones que abren el contenido esencial del mismo. Dentro de las mismas, podemos observar algunas cuestiones a modo de aclaración. La primera consideración recoge que “La protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental”: como ya sabemos es un derecho fundamental que responde al poder de la globalización y a la informatización de nuestros datos.

Aunque dentro de la red social no existan fronteras delimitadas, los usuarios que las conforman, están protegidos por un derecho positivo sobre posibles conflictos. Y ante esto, existe una novedad de gran importancia. Hablamos del ámbito de aplicación territorial, ya que afecta a todos los responsables que estén ubicados en territorio de la UE, pero además, ahora también afecta a todos aquellos que traten con datos de personas europeas, aunque la sede donde se traten los datos, esté en otro país no integrante de la UE. Existe un auto del TS donde podemos observar que será de las últimas veces que se plantee un problema en cuanto al ámbito de aplicación. Se trata del recurso de casación 627/2018, en el que se presenta una sanción impuesta por la AEPD a una persona y se discute el ámbito de aplicación ya que realmente la empresa a la que esta persona está adherida no tiene el centro de sus intereses en España. Con el nuevo reglamento, por el simple hecho de tratar datos personales de ciudadanos y ciudadanas europeos y europeas, ya será de aplicación el mismo.

Esto supone un refuerzo a la protección, que abarca a partir de ahora, a cualquier sujeto de la UE sin importar dónde se traten sus datos[35]. Hasta ahora, el argumento que sostenían las empresas que trataban datos de personas europeas para no cumplir con la normativa era no tener la sede en Europa y, por tanto, estar exentas de obligaciones.

El experto ÁNGEL BENITO RODERO, abogado especialista en Internet y delegado de protección de datos, explica las novedades más importantes que introduce el nuevo Reglamento, centrándose en las siguientes[36]: por un lado, el Derecho a no ser objeto de decisiones automatizadas, se exige al menos que exista una intervención humana; la obligatoriedad de comunicar a la autoridad de control las violaciones que se produzcan a la seguridad de los datos personales, las llamadas "brechas de seguridad"; el nuevo derecho de portabilidad de los datos; la creación de un Comité de protección de datos europeo; y la introducción de una sanción administrativa del 4%.

Empezando por la primera de ellas, el artículo 22 da respuesta a un problema con el que nos podemos encontrar todos a la hora de "hablar con una máquina". Se reconoce expresamente el derecho de no ser objeto de una decisión tomada por un tratamiento únicamente automatizado que produzca efectos jurídicos o similares. En este sentido, el *Big Data* vuelve a ser objeto de análisis en cuanto a cuestiones jurídicas. Un ejemplo claro anterior a la aparición del *Big Data* son las entidades bancarias, que han utilizado siempre como referencia para conceder un crédito, las probabilidades de que el sujeto lo devuelta[37].

La toma de decisiones exclusivamente automatizada es el poder de tomar decisiones por medios tecnológicos sin que medie ninguna intervención de carácter humano. Las decisiones automatizadas pueden basarse en muchas clases de datos, desde datos recogidos en un cuestionario hasta datos

[35] Revista de prensa, *El reglamento de protección de datos en 12 preguntas*. Disponible en: *http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2016/notas_prensa/news/2016_05_26-ides-idphp.php*

[36] Entrevista Ángel Benito Roderó, 16 de abril de 2018, 09:00 h "Hub" Salamanca

[37] VIOLANTE, M. 5 cosas en las que se fijan los bancos al dar créditos. Disponible en: https://www.entrepreneur.com/article/268358

producto de observaciones sobre los individuos, como puede ser el caso de los datos sobre ubicación, recopilados a través de una aplicación como una red social[38].

Como hemos señalado en numerosas ocasiones, los avances en la tecnología vuelven a ser protagonistas aquí junto a las capacidades de análisis de *Big Data*, inteligencia artificial y aprendizaje automático. Todo ello junto ha permitido la facilidad para crear perfiles y tomar decisiones automatizadas pudiendo afectar significativamente los derechos y libertades de las personas[39].

La información que se encuentra disponible sobre los datos personales en el marco de dispositivos sobre Internet y la capacidad de identificar correlaciones y crear enlaces permite determinar, analizar y predecir aspectos de la personalidad o el comportamiento de un individuo, sus intereses y sus hábitos.
La creación de perfiles y la toma de decisiones automatizada pueden ser útiles para individuos y organizaciones, proporcionando beneficios múltiples como el ahorro de recursos para un proceso electivo, pero a la vez supone una vulneración muy grande del derecho fundamental de la protección de datos a las personas que son objeto de tales decisiones[40].

Una empresa puede querer elegir a sus trabajadores en función de aspectos concretos. El reglamento no incluye en qué momento se considera que un tratamiento únicamente automatizado está afectando a una persona, pero es cierto que si para crear un perfil una empresa utiliza estos mecanismos, se pueden asociar comportamientos erróneos a personas[41]. Únicamente se refiere a que produzca efectos jurídicos o similares. Cabe la posibilidad de que este tratamiento derive en la proliferación de estereotipos cuando el perfil se crea con características como, por ejemplo, la raza o la religión, suponiendo sesgos

[38] Article 29 data protection Working 2018. p.8
[39]Article 29 Data Protection Working *Op.cit* p.5
[40] Article 29 Data Protection Working *Op.cit* . p.5
[41] GIL, E. *Cuando al robot no le gusta tu barrio*, Cuestiones delBig Data. *Blog Legal Today*. 2017.

discriminatorios[42]. Puede desembocar tanto en la denegación de servicios y bienes, comoen una discriminación injustificada.

El Reglamento introduce nuevas herramientas para abordar los riesgos que surgen de la creación de perfiles y la toma de decisiones automatizada, en particular el relativo a la privacidad. La fuente de la que emana esta problemática puede extenderse tanto al campo de creación de perfiles en una empresa que demanda mano de obra, como para una empresa que busca perfiles determinados a los que ofrecer sus productos, lo que se denomina mercadotecnia directa. De cualquier modo, el artículo 21 recoge el derecho de oposición a ser objeto de decisiones automatizadas dentro de las que se encuentra la elaboración de perfiles. El problema es que no se concibe como un derecho absoluto, que faculta al responsable del tratamiento de datos a seguir usándolos si acredita motivos legítimos imperiosos[43].

A cualquier herramienta podemos darle un uso adecuado o inadecuado, por lo que cuando estamos hablando de situaciones jurídicas o similares que afecten a las personas, es necesario que exista una intervención humana que armonice la automatización en su sentido más extremo.

El problema más importante es que este derecho solo se puede ejercitar, cuando la persona sabe que es objeto de decisiones únicamente automatizadas, y en la mayoría de los casos se ignora este hecho[44]. El caso más común en el que nos damos cuenta de este tratamiento se produce cuando tenemos una incidencia que comunicar a una empresa, que además nos afecta, como cuestiones de pago ante compañías telefónicas, y nos resulta imposible hablar con una persona para solucionarlo.

En cuanto a la obligatoriedad de comunicad las “brechas de seguridad” a la autoridad de control, la encontramos contemplada en el artículo 33 de este

[42] COTINO, L. “*Big Data e inteligencia artificial*”, Una aproximación a su tratamiento jurídico desde los derechos fundamentales , Dilemata, 2017, p. 1.
[43] ÁLVAREZ, M. *Reglamento general de protección de datos: Hacia un nuevo modelo europeo*. Madrid 2016 p.236
[44] Entrevista Ángel Benito Roderó, 16 de abril de 2018, 09:00 h “Hub” Salamanca

Reglamento UE 2016/679. En España, la autoridad de Control es la AEPD, a la que se deberá notificar cualquier violación en la seguridad de los datos en un periodo no superior a 72 horas[45]. En dicha notificación deben ir incluidos una serie de aspectos aportados por el responsable, tal como señala el apartado 3 del mismo artículo.

Se debe describir la naturaleza de la violación de seguridad, así como el nombre y los datos de contacto del delegado de protección de datos, la descripción de las posibles consecuencias de la "brecha de seguridad" y las medidas adoptadas por el responsable del tratamiento para los efectos de la misma. Si por cualquier motivo, la notificación se hiciera posteriormente, se debe justificar el porqué. Es un tema de una importancia muy grande, ya que hoy en día las empresas usan armas de *hackeo* para sabotearse entre ellas, y al fin y al cabo la diana se encuentra centrada en los datos de las personas[46].

En el artículo 34, se contempla la posibilidad de comunicar al interesado la brecha, en el caso de que la violación de seguridad suponga un alto riesgo para el mismo. Solo se puede prescindir de esta comunicación cuando, el responsable, ha adoptado medidas para neutralizar los efectos de la violación. Aquí la autoridad de control vuelve a tener un papel fundamental, pues es la encargada de instar al responsable para que comunique esta situación al interesado, si no lo ha hecho, y considera que sigue suponiendo un alto riesgo. Realmente, una de las novedades importantes es la actuación previsora que se introduce, sin importarle al Reglamento el formato en el que se contengan los datos (automatizado o no), pues el único propósito es la seguridad de los mismos.

Es decir, a parte del protocolo a seguir cuando se produzca una "brecha de seguridad", también se exige de manera añadida, la adopción de medidas preventivas. En el artículo 35 se recoge la herramienta de la "*evaluación de impacto relativa a la protección de datos y consulta previa*". Su fin es proteger los datos de tratamientos, que más probablemente, puedan poner en peligro

[45] FERNÁNDEZ, E. *Op.cit.* p.32

[46] Entrevista Ángel Benito Roderó, 16 de abril de 2018, 09:00 h "Hub" Salamanca

derechos y libertades de las personas[47]. Se recoge expresamente "*si utiliza nuevas tecnologías*", por lo que si un tratamiento se lleva a cabo por una red social, o utilizando el *Big Data*, debe contener esta evaluación de impacto. Estas medidas son de suma importancia también en el campo de la sanidad[48].

En relación a la mención anterior del artículo 22, hay que introducir la no discriminación de la que hablábamos, en la evaluación de impacto de protección de datos, ya que sobre el resultado del tratamiento de los datos de una persona determinada, se toman decisiones que le afectan jurídica o similarmente[49]. Son herramientas de prevención porque su finalidad es evitar que se produzca un perjuicio, entre ellas también encontramos las del artículo 25 "Protección de datos desde el diseño y por defecto".

Dentro de las novedades también encontramos el derecho a la portabilidad de datos, que está relacionado con el importante derecho al olvido, en el Reglamento podemos situarlo desde el artículo 15 al 23. El artículo 17 recoge expresamente el derecho al olvido, dándole al interesado el poder de decidir suprimir los datos, comunicándolo al responsable del tratamiento, si los datos ya no son necesarios en relación con el fin para el que se recogieron, además de si retirase su consentimiento o si los datos se hayan tratado de manera ilícita[50]. Es muy importante que este artículo en su segundo apartado intente minimizar los daños del efecto multiplicador que lleva implícito Internet, por lo que si el interesado ejerce su derecho al olvido, se ejerce tanto hacia el que ha tratado sus datos como a sus efectos sobre terceros que puedan acceder a ellos[51].

Es importante mencionar al respecto, la sentencia del Tribunal de Justicia de la Unión Europea, Gran sala, de 13 de mayo de 2014 contra *Google*, relativa al derecho al olvido. La importancia radica en que cuando accedemos a Internet y

[47] GARRIGA DOMÍNGUEZ, A., *Nuevos retos para la protección de datos personales en la Era del Big Data,* Dykinson, Madrid, 2016, p.246
[48] PRIETO HERGUETA, J., *Guías y herramientas de apoyo para adaptarse al RGPD*. *Informática y salud* ISSN 1579-8070, núm. 127, 2018 p. 28-30
[49] COTINO, L. *Op.cit.* p. 139.
[50] FERNÁNDEZ, E., RGPD: *Seguridad, privacidad y oportunidad de negocio, Redseguridad* núm. 78, 2017, p.32-33
[51] CHÉLIZ, MºC. *Op. cit.* p.262

a plataformas como redes sociales, dejamos en cierta manera un rastro de actividad[52]. Se trata de una cuestión prejudicial que se planteó ante el tribunal en el seno de una reclamación estimada por parte de la AEPD, en la que el Sr. Costeja solicitaba a *Google* que quitase la información privada que aparecía en el motor de búsqueda al introducir su nombre, ya que se contenían datos de un embargo que había sufrido. Se plantean numerosas cuestiones como el tiempo transcurrido o incluso hasta dónde llega la responsabilidad del responsable del motor de búsqueda, pero queda claro que el Sr. Costeja tiene derecho a que una subasta no esté vinculada a algo tan personal como lo es su nombre[53].

Encontramos una ST del TS 3166/2017 Sala de lo Civil, bastante reciente que aborda este problema, reconociendo el derecho de la parte actora a cancelar los datos relativos a los ficheros que la calificaban de "morosa" y a los que se podía acceder fácilmente. Textualmente hablan de las consecuencias que puede ocasionar como una realidad "consecuencias que la inclusión de sus datos en los registros de morosos tuvo para la demandante, tanto de orden moral como patrimonial".

El derecho a la portabilidad de los datos está íntimamente relacionado ya que entra dentro del derecho al olvido, pero además, faculta al solicitante a llevarse todos sus datos consigo, como señala el artículo 20 del Reglamento. Supone un avance ya que, de esta manera, los usuarios podrán solicitar en cualquier momento todos los datos que existen acerca de ellos y que están contenidos en la plataforma virtual. Esta idea emana de un caso mediático en el que un abogado austriaco inició diligencias contra *Facebook* solicitándole que le enviase todos los datos que tenía sobre él y se sorprendió cuando a su domicilio llegaron 1200 páginas con todos sus datos. La Sentencia del Tribunal de Justicia, Gran sala, de 6 de octubre de 2015, recoge este caso en el que se invoca una cuestión prejudicial a tenor de los artículos 7,8 y 47 de la Carta de los Derechos fundamentales de la Unión Europea y los artículos 25 y 28 de la Directiva 95/46/CE. Se reconoce que las prácticas que se realizan a la

[52] ESCRIBANO, P. *Op.cit.* p.72
[53] BERROCAL, A. *Op.cit* p.157

protección de datos personales no son válidas[54]. Es un caso que ha impulsado en cierta manera todos estos cambios[55].

Todo ello es necesario, debido a que la tecnología y su avanzado desarrollo, hacen posible encontrar datos personales de cualquier persona en cuestión de segundos, información que muchas personas desean borrar o suprimir, por ejemplo: un abogado puede verse sufriendo las consecuencias de una sentencia de estafa que vincula a su hermana[56].

Es un aspecto que trasladamos a las redes sociales, el derecho al olvido digital, que se ejercita de la misma forma para proteger la privacidad en Internet y es por lo que este derecho se presenta como una manifestación del derecho fundamental a la protección de datos personales[57]. Pueden existir conflictos de intereses, como por ejemplo un conflicto con el derecho a la libertad de expresión. En definitiva, supone un problema si no se aplica correctamente ya que las nuevas generaciones pueden verse muy afectadas por las publicaciones que han realizado en las redes sociales, pudiendo hipotecar su futuro por el recuerdo permanente de su ayer[58]. En el reglamento europeo se han incrementado sustancialmente las infracciones y las sanciones, pero especialmente encontramos que el reglamento se encuentra intentando armonizarse con el entorno de Internet para que las personas puedan ejercer un mayor control en la era del *Big Data*[59].

Aquella persona que haya sufrido un perjuicio, material o inmaterial, a causa de una operación de tratamiento de sus datos, que no haya realizado conforme a la normativa tiene derecho a acudir ante la autoridad de control y presentar una

[54] InfoCuria – Jurisprudencia del Tribunal de Justicia. Sentencia del Tribunal de Justicia (Gran Sala) de 6 de octubre de 2015. Disponible en: http://curia.europa.eu/juris/document/document.jsf?docid=169195&doclang=ES

[55] PAGINA DE PRENSA Alto nivel. 16 de Mayo 2018. Disponible en: https://www.altonivel.com.mx/actualidad/internacional/dolor-de-cabeza-a-mark-zuckerberg/

[56] COTERA, J.: *Relato del VII Congreso Internacional sobre Internet, Derecho y Política: Neutralidad de la red y derecho al olvido*, *IDP. Revista de Internet, Derecho y Política*, núm. 13, 2012, p. 89

[57] GARRIGA DOMÍNGUEZ, A. *Op.cit* p.239.

[58] CHÉLIZ, MºC. *Op. cit.* p.268

[59] ÁLVAREZ, M. *Op. cit.* p.249

reclamación. La sanción irá en relación al artículo del Reglamento que se haya vulnerado, que puede ascender desde los 10 millones de euros o el 2% como máximo del volumen de negocio total anual, hasta los 20 millones de euros o el 4% como máximo del volumen de negocio anual. Esto supondrá una sanción importante sobre todo para las grandes empresas[60]. Por último, dentro de este punto, como ya destacamos en varias ocasiones la AEPD tiene potestad sancionadora que va a verse acrecentada por la aplicación del reglamento. La AEPD se ha pronunciado en temas importantes en este sentido, como las tres sanciones que se impusieron a *WhatsApp* por el intercambio de datos entre esta y *Facebook*, siendo la única autoridad europea en hacerlo con una multa que ascendía a los 300.000 euros a cada red social[61].

Nos introducimos ahora en la creación del Comité Europeo de Protección de Datos. En el artículo 68.1 del Reglamento, encontramos la mención a la creación del Comité, quien tendrá personalidad jurídica. En este sentido, y en relación a la consideración 139 del reglamento, esta figura viene a sustituir al Grupo de protección de las personas creado por la directiva 95/46/CE el conocido Grupo de trabajo del artículo 29 (GT29).

Es el artículo 70.1 del reglamento el encargado de recoger y detallar las funciones del Comité. Como funciones principales encontramos la de supervisar y garantizar la adecuada aplicación del RGPD, también el comité tiene la función de asesoramiento a la Comisión sobre las cuestiones relativas a la protección de datos, como las propuestas de modificación del mismo reglamento o sobre los procedimientos para intercambiar información entre los responsables.

También se le encarga la tarea de emitir directrices, recomendaciones y buenas prácticas con el bien de concretar aún más, los criterios y requisitos de las decisiones basadas en perfiles creados de manera automatizada, además

[60] MUNDO LOPD, *Infracciones y sanciones en el RGPD,* 2018. Disponible en: http://www.mundolopd.com/lopd/infografia-infracciones-sanciones-reglamento-general-proteccion-datos/

[61] PERIODICO DE NOTICIAS El país. *Mar España: "Seremos beligerantes con todas las redes sociales*". 24 Mayo 2018. Disponible en: https://elpais.com/economia/2018/05/22/actualidad/1527003631_400767.html

de constatar las violaciones de la seguridad y dictaminar si ha existido una dilación indebida por parte del responsable. Cabe mencionar que existen otras funciones asignadas al comité en relación a la comisión como el mandato de facilitarles un dictamen sobre los requisitos de certificación. Un aspecto muy importante es que sus debates gozarán de confidencialidad siempre que el mismo lo considere oportuno o que se haya establecido previamente. Este comité actúa con independencia, es decir, en su jerarquía no admitirá ni solicitará instrucciones o directrices de nadie, ni sobre sus funciones ni sobre el desarrollo de sus competencias. El propio RGPD recoge cual será la estructura interna que estará formada por un presidente, un director de cada autoridad de control de cada estado miembro, un supervisor europeo y una secretaría[62].

El experto JORGE GARCÍA HERRERO, abogado, delegado de protección de datos y especialista en digitalización y nuevas tecnologías, habla como novedad más importante acerca de los matices que el RGPD introduce en cuanto al consentimiento [63] . Dicho consentimiento debe ser granular o vertebrado y explícito, específico en vez de en bloque, y tiene que ser prestado por el titular de manera libre entendiéndose por qué no lo es cuando el mismo sufre un perjuicio cuando lo presta o cuando el desequilibrio de poder está presente. Podemos encontrar numerosos llamamientos a como debe ser el consentimiento dentro del reglamento, como el artículo 6, el artículo 7 o en la consideración nº11. En cierta manera se intenta nivelar la desigualdad innegable que existe entre los interesados y los responsables del tratamiento[64].

El gran problema que plantea el uso no controlado de los menores en las redes sociales, se ve respondido en el Reglamento Europeo en este sentido: *"*Si el niño es menor de 16 años, tal tratamiento únicamente se considerará lícito si el consentimiento lo dio o autorizó el titular de la patria potestad o tutela sobre el niño, y solo en la medida en que se dio o autorizó*",* recogido en el artículo 8 del

[62] MORALES MARTÍN, T *Funciones del nuevo Comité Europeo de Protección de Datos* 2017 disponible en: https://www.prodat.es/blog/funciones-nuevo-comite-europeo-proteccion-datos-parte-ii.html

[63] GARCÍA HERRERO, J, *Reglamento Europeo de Protección de Datos: Guía Resumen*, 2017 disponible en: http://jorgegarciaherrero.com/reglamento-europeo-de-proteccion-de-datos-breve-guia-de-uso/

[64] GARRIGA DOMÍNGUEZ, A. *Op.cit* p.236

Reglamento Europeo relativo a las Condiciones aplicables al consentimiento del niño en relación con los servicios de la sociedad de la información.

Se explica también, que los consentimientos de ayer, es decir, los prestados por los usuarios que no cumplan con los requisitos de hoy del RGPD, no serán válidos. En este sentido es importante traer a colación la famosa lista *Robinson*[65]. Se trata de una lista en la que un usuario debe inscribirse si no desea que una compañía telefónica use sus datos que no ha consentido para ofrecerle una serie de productos o servicios. Realmente se vende como algo positivo, que beneficia a las personas para que no reciban estas llamadas, pero la verdad es que nadie concibe la idea de inscribirse en una lista para que no vulneren su derecho a la vida o a tener una vivienda digna porque son derechos fundamentales. El derecho a la protección de datos también lo es, por lo que no deberíamos inscribirnos a una lista para que respeten un derecho que de por sí deberían respetar. Con el RGPD y lo concerniente al consentimiento que hemos nombrado, en teoría no debería vulnerarse el derecho a la protección de datos de carácter personal a ninguna empresa a la que no se le ha prestado el consentimiento explícito, consciente y libre.

Este experto también trata los y las DPD como una novedad introducida por el RGPD, ya que se trata de un perfil nuevo adjunto a la protección de datos personales con importantes ocupaciones y responsabilidades. Su tarea principal radica en asesorar al responsable del tratamiento sobre lo que hay que hacer, supervisar el cumplimiento de la normativa por parte de su cliente y explicar al personal cuáles son sus obligaciones en cuanto a la protección de datos. Realmente se limita a explicar lo que debe hacerse y de qué manera, pero es la empresa y el responsable del tratamiento quienes deben llevarlo a cabo. Esta figura puede ser encarnada por un trabajador o trabajadora de la empresa, por un jurista, por un tecnólogo o tecnóloga y puede ser una persona física o jurídica e, incluso, puede atender a varias organizaciones. Lo más importante acerca del DPD es que será el interlocutor entre la empresa y la

[65] BUISÁN, N. *La ley de protección de datos. Análisis y comentario de su jurisprudencia.* En Carlos Lesmes Serrano. (coord.) 2008. p.537

autoridad de control que en España como ya hemos dicho es la AEPD en caso de denuncia, inspección o comunicación de brecha de seguridad.

También esta figura está capacitada para recibir reclamaciones, nos referimos a las reclamaciones que se pueden presentar contra una organización y que pueden hacerse frente a la AEPD o ante el o la DPD, con el resultado de que puede terminar desempeñando funciones propias de un mediador entre la organización o empresa y el interesado afectado. Destaca también la responsabilidad proactiva, el llamado *Accountability*. Se trata de imponer la obligación a las organizaciones de aplicar una responsabilidad activa, es decir, por la que se cumpla la normativa del RGPD de manera activa cumpliendo y demostrando que se cumple la norma. El hecho de demostrar que se cumple la norma se hace posible mediante la imposición de establecer una autoevaluación de riesgos, de comunicación de brechas de seguridad y demás medidas preventivas que ya se han nombrado anteriormente.

Por último, el RGPD aborda el interés legítimo. La protección de datos de carácter personal está basada en el consentimiento del interesado, pero en ocasiones, es posible tratar datos sin dicho consentimiento. Entre ellas, el interés público, la protección de un interés vital del interesado como una urgencia médica o bien el interés legítimo, que en muchas ocasiones supone un reto identificar qué entendemos exactamente por interés legítimo sobre todo en una red social donde hoy en día estamos acostumbrados a considerar que toda información "pública" es lícita compartirla y explotarla. Además, en el sector jurídico se encuentra otro dilema relativo a este tema, que es el del interés público que tienen las sentencias contra el derecho fundamental de la protección de datos. La AN ha recogido en ST 9 de julio de 2009 que queda condicionado el derecho a la libertad de información del artículo 20.d CE a que se hable de cuestiones de relevancia pública y que además sea contenido veraz[66].

[66] HEREDIA, N. *Publicación de sentencias: Protección de datos vs interés público*. Disponible en: http://www.legaltoday.com/practica

4. Breve referencia al Anteproyecto de Ley Orgánica de protección de datos de carácter personal

Lo que se hace en el Anteproyecto es adaptar la normativa del RGPD directamente en el derecho español. La nueva Ley Orgánica de protección de datos de carácter personal derogará a la Ley 15/1999 de 13 de diciembre, de protección de datos de carácter personal y que ha sido objeto de análisis en el presente trabajo. Las novedades que se introducen en el anteproyecto con respecto al RGPD son: las referentes al consentimiento y el consentimiento de menores, las cuestiones relativas a personas fallecidas, la licitud del tratamiento e interés legítimo, la transparencia e información, el derecho a la portabilidad, la designación de delegado de protección de datos evaluación de impacto y el régimen sancionador. En cuanto al consentimiento, recogido en el artículo 7 del Anteproyecto y en el artículo 7 del RGDP, se clarifica que no cabe el consentimiento tácito, sino que ha de ser un consentimiento libre, específico, informado y que se haga mediante una clara acción afirmativa.

Además, se añade que debe recabarse un consentimiento por cada una de las finalidades para las que se recogen los datos de carácter personal. Dentro de este tema, encontramos el consentimiento de menores, en el artículo 8 del anteproyecto en relación al artículo 8 del RGPD [67]. En este sentido, el anteproyecto fija la edad mínima en los 13 años ya que, aunque en el RGPD la edad mínima para prestar consentimiento a cerca de los datos de los menores es de 16 años, se deja un margen de libertad a los estados miembros.

En cuanto a las personas fallecidas, el artículo 3 del Anteproyecto aplica las consideraciones 27, 158 y 160 del RGPD en el sentido de que establece que los herederos puedan ejercer los derechos de acceso, rectificación o supresión en nombre de una persona que ya haya fallecido.

[67] IAB SPAIN, *Asociación de la publicidad, el marketing y la comunicación digital en España.* Disponible en: https://iabspain.es/wp-content/uploads/principales-aspectos-del-anteproyecto-lopd-iab-spain-1.pdf

Acerca de la licitud del tratamiento y el interés legítimo, los artículos del 12 a 20 del Anteproyecto adaptan el artículo 6 del RGPD, expresando que puede procederse a incluir en interés legítimo, por ejemplo, en sistemas de exclusión publicitaria o video vigilancia en la empresa. En cuanto a la video vigilancia dentro de una empresa, se presenta como interés legítimo el hecho de querer protegerse frente ataques o actitudes ilícitas que puedan perjudicarla y para lo que es necesario grabar a los trabajadores en sus puestos de trabajo[68].
Por otro lado, la transparencia e información que encontramos en el artículo 21 del Anteproyecto y que vienen a aplicar los artículos 12, 13 y 14 del RGPD porque se establece la oportunidad de informar por capas, que se traslada además a la elaboración de perfiles creados de manera automatizada, dándole oportunidad al afectado de oponerse a ello siempre que esa decisión pueda producirle efectos jurídicos o pueda afectarle de manera importante.

En el tema de la portabilidad de datos, el Anteproyecto solo hace referencia a los datos facilitados por el afectado y los derivados directamente del uso de los servicios prestados por el responsable. El artículo 27 del Anteproyecto se ocupa de ello, excluyendo los datos inferidos que son aquellos que se deducen de los datos que previamente un interesado ha prestado, estos datos inferidos sí se tienen en cuenta en el artículo 20 del RGPD.

Para la designación de DPD los artículos 35 a 37 del proyecto de Ley, establecen 15 casos en los que el nombramiento es obligatorio, sumando algunos casos que no se encuentran en el RGPD en sus artículos 37, 38 y 39. En este sentido, se incluye que las redes tienen que nombrar obligatoriamente a un DPD, el motivo viene dado por el uso intensivo y a gran escala de los datos, que llevan a cabo las redes sociales [69].

[68] GARCÍA HERRERO, J, disponible en: http://jorgegarciaherrero.com/reglamento-europeo-de-proteccion-de-datos-breve-guia-de-uso/
[69] Revista de prensa, *AEPD publica un sistema de notificación electrónica para comunicar la designación de Delegados de protección de datos*. Disponible en: https://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2018/notas_prensa/news/2018_04_10-ides-idphp.php

Se exige nombrar un DPD incluso a los detectives privados, por el uso intensivo de los datos, normalmente sobre la vida sexual de las personas que investigan[70].

La evaluación de impacto se incluye como una obligación del responsable y el encargado cuando, por ejemplo, se desarrollen actividades de publicidad. Por último, el régimen sancionador se incluye en el anteproyecto en la directriz de establecer una graduación de infracciones en leves, graves y muy graves.

IV. LAS POLÍTICAS DE PRIVACIDAD DE LAS REDES SOCIALES

1. Análisis de las condiciones de las políticas de privacidad de las redes sociales. Caso *Instagram*

1.1. Condiciones políticas de privacidad de 2013 a fecha de marzo

En este punto vamos a analizar directamente las condiciones que se encuentran recogidas en las políticas de privacidad de las redes sociales, en concreto las que se encuentran en la red social *Instagram* (ver Anexo 1), por su creciente importancia en el mundo de las redes y por qué fue adquirida en 2012 por *Facebook*, un gigante de las redes sociales. Su política de privacidad entró en vigor el 19 de enero de 2013, que tiende más a la autorregulación que a adaptarse a una normativa concreta, dándose así varios problemas[71]. En una primera lectura, observamos que aún a fecha de marzo del presente año no habían actualizado sus políticas a lo que exige el RGPD, que entró en vigor en 2016, tres años después de que entrasen en vigor sus políticas de privacidad.

Pero si bien es cierto que recoge un apartado llamado "*cookies y tecnologías similares*" donde advierten que al dar el consentimiento de uso de la aplicación, pueden solicitar a anunciantes que envíen publicidad a tu dispositivo. Esa

[70] *Blog de protección de datos.* Disponible en: https://www.protecciondatos-lopd.com/empresas/normativa-detectives-privados/
[71] TRONCOSO, A*. Op.cit* p.37

publicidad será de productos o tendencias similares a las que como usuario visitas cada día. Es una aplicación directa del *Big Data*. Contiene un punto en su política titulado "*Cómo utilizamos tu información*" en la que pueden utilizar la información recibida, por ejemplo, "*proporcionando información que puede incluir anuncios de Internet y otros formatos de marketing*". Se nos advierte, además, que nuestra información como usuarios se puede recopilar o procesarse en los Estados Unidos o donde *Instagram* tenga sus filiales.

Llegados a este punto exacto, encontramos algo que el RGPD va a evitar de lleno. *Instagram* pone de manifiesto cómo la propia red socal, sus filiales o proveedores de servicios pueden transferir la información que se recopile de los usuarios. Se incluye la información personal que tenga tanto en sus países como en otros. En cambio, si ese usuario se encuentra en la UE informan explícitamente "*ten en cuenta que podemos transferir la información, incluida la de carácter personal, a un país y una jurisdicción que no tengan las mismas leyes de protección de datos que tu jurisdicción".* El RGPD debe aplicarlo cualquier empresa, red, sociedad, que maneje datos personales de ciudadanos europeos, sea donde sea que tengan su sede.
Tampoco mencionan el nombramiento del DPD, que como hemos explicado en puntos anteriores, es estrictamente obligatorio para aquellos que hacen un uso intensivo y a gran escala de los datos de carácter personal. Cuando lo lleven a cabo, deben aceptar todas las recomendaciones que éste le haga y adaptarse al RGPD en todos sus demás aspectos y novedades. *Instagram* declara claramente cómo, aunque dicen intentar establecer protección a la seguridad, no se hacen cargo de garantizar la seguridad de la información que cada usuario transfiera a *Instagram*. De igual modo, no se hace cargo de que toda la información de los usuarios pueda modificarse o divulgarse.

A partir del 25 de mayo del presente año, *Instagram* ya debe hacerse cargo totalmente de la seguridad de los datos a los que dan tratamiento, al menos de los ciudadanos europeos, comunicando las famosas "brechas de seguridad" a las que nos hemos referido anteriormente. La información que se da sobre su política de privacidad no se presenta en absoluto de una manera fácil de leer,

sino que debe ser más clara, más resumida y en un lenguaje comprensible para las personas que la lean la entiendan.

Por último, el derecho a la portabilidad de datos, no se encuentra tampoco reconocido, pero además se menciona que cuando un usuario cierra su cuenta, pueden contener los datos del mismo el tiempo que consideren oportuno y razonable.

Una cuestión de vital importancia es que tampoco se encuentran mecanismos de verificación de la edad de los menores, mecanismos que según MAR ESPAÑA se encuentran a disposición de las redes sociales que lo deseen como la verificación mediante la introducción del Documento Nacional de Identidad[72].

1.2. Política de Privacidad a fecha de mayo de 2018

La política de privacidad en sí misma se encuentra en estado de modificación. *Instagram* advierte que se están realizando cambios para adaptarse al reglamento, pero han anunciado que están trabajando en crear un nuevo instrumento que permitirá a los usuarios y usuarias descargar todos los datos que hayan compartido en la red social hasta el momento, como videos, fotos y mensajes[73]. Supone un avance en cuanto al derecho de portabilidad de datos que ya enuncia el RGPD.

2. Estudio del consentimiento del usuario en sus políticas de privacidad

2.1. El consentimiento a fecha de marzo de 2018

[72] PERIODICO DE NOTICIAS El país. *Mar España: "Seremos beligerantes con todas las redes sociales*". 24 Mayo 2018. Disponible en: https://elpais.com/economia/2018/05/22/actualidad/1527003631_400767.html

[73] PAGINA DE PRENSA La Vanguardia. *Instagram ofrecerá la posibilidad de descargar los datos compartidos.* 14 de Mayo 2018 Disponible en: http://www.lavanguardia.com/tecnologia/20180414/442488572158/instagram-privacidad-protecion-de-datos.html

En cuanto al consentimiento, tampoco se ha adecuado al RGPD, porque no se presenta de manera vertebrada, específica ni concreta. No se aseguran por tanto, de que todos sus usuarios hayan entendido los fines para los que consienten. Si preguntásemos al azar a 1000 personas que utilizan esta red social, si saben que con sus datos se puede "comerciar", seguramente la gran mayoría nos diría que lo desconocen. La red social debe asegurarse de que el consentimiento es informado y válido, para lo que deben presentar de forma transparente, los reales fines para los que utilizan los datos.

Al no haberse actualizado a mes de marzo de 2018 las políticas conforme al RGPD, podrían encontrarse con problemas como en el que se vio inmerso *Facebook* pues, como hemos dicho anteriormente, *Instagram* fue adquirida por *Facebook* y comparten políticas de privacidad. El conflicto en cuestión es el caso de *Facebook y Cambridge Analytica*. Christopher Wylie, creó un método que esta última empresa utilizó. La misma se dedicada a la supersegmentación publicitaria estudiando perfiles psicológicos, ayudando a las empresas a vender productos a un público específico previamente estudiado. El estudio de estos datos se utilizó para favorecer incluso campañas políticas, a las que les beneficiaba este método para influir en los votantes. Realmente todo esto fue posible debido a que *Facebook* se nutre de la publicidad por la que gana dinero, con lo que se acabó por vender datos a terceros para mostrar una publicidad selecta adaptada a cada persona[74].

El verdadero problema, se plantea desde el punto de vista de cómo se obtuvieron estos datos. En el año 2014, *Cambridge Analytica* creó un test de personalidad que introdujo en *Facebook* y que de cara a las personas que lo realizaban, se trataba de un test interesante sin trasfondos. Realmente, podemos afirmar que se trataba de un caballo de Troya, puesto que para realizarlo, las personas autorizaban sin ser conscientes de su finalidad, que Cambridge accediera a sus datos y a los de sus amigos. El diseño de

[74] PERIODICO DE NOTICIAS El país. *Mar España: "Seremos beligerantes con todas las redes sociales*". 24 Mayo 2018. Disponible en: https://elpais.com/economia/2018/05/22/actualidad/1527003631_400767.html

seguridad de *Facebook* permitió que esto se llevase a cabo sin “brechas de seguridad”, pues no se hizo mediante un *hackeo*.

Facebook al ser consciente, solicitó que *Cambridge Analytica* borrase los datos, cuestión prácticamente imposible dado que ya estaban en toda la red. Todo este asunto ha derivado en que estos datos que se recogieron, sirvan a empresas para crear perfiles psicológicos y se ha llevado a cabo sin el consentimiento lícito de los usuarios[75].

Es desmesurado el uso que se hace de los datos, ya que todas las personas que usan este tipo de red social lo hacen como actividad lúdica y de sociabilización, desconociendo en todo momento que el tratamiento de sus datos se compra y se vende en un mercado ajeno para los propietarios de esos datos. Esto se denomina mercadotecnia directa como ya apuntábamos, a la que los usuarios deberán poder negarse, ejercitando el derecho que recoge el artículo 21 del RGPD[76].

En marzo de 2018, *Instagram* no tenía configurado el consentimiento de tal manera que los usuarios pudieran ejercitar el nombrado derecho y oponerse a estas operaciones. Lo que se trata de conseguir es que el consentimiento no sea estático sino activo, que no sea un bloque entero en el que los usuarios no tengan otro remedio que aceptarlo por entero.

En el momento en el que adecuen todo lo relativo al consentimiento, deberán en teoría, eliminar los métodos anteriores porque como nos recordaba el experto JORGE GARCÍA HERRERO, los consentimientos prestados que no cumplían el RGPD no serán válidos. Se recoge como pueden hacer cambios en las políticas de privacidad periódicamente, por lo que recomiendan que se lean con frecuencia. Esto violaría por completo el consentimiento prestado en un principio por los usuarios, porque conlleva que se pueden hacer cambios y se sobreentiende que los usuarios aceptan sean cuales sean.

[75] GONZALEZ M. Disponible en: https://www.xataka.com/legislacion-y-derechos/que-ha-pasado-con-facebook-del-caso-cambridge-analytica-al-resto-de-polemicas-mas-recientes
[76] DPO&It Law. Disponible en: http://www.dpoitlaw.com/reglamento-general-de-proteccion-de-datos-rgpd-derecho-de-portabilidad-oposicion-y-a-limitar-las-decisiones/

2.2. El consentimiento a fecha de mayo de 2018

Al igual que en el apartado anterior, no encontramos un cambio sustancial en lo concerniente al consentimiento, si bien es cierto que existe un espacio destinado a prestar el consentimiento para que las marcas etiqueten el perfil de los usuarios. Es decir, solo si las personas hacen un consentimiento expreso pulsando un botón que se habilita para ello, las marcas tendrán derecho a etiquetar a los mismos en sus contenidos. No estamos ya ante un consentimiento tácito en el sentido de aceptar un bloque uniforme acerca de toda una política que antes no cabía ir aceptando por partes.

V. CONCLUSIONES

A la luz de lo estudiado acerca de la protección de datos de carácter personal, sobre cómo afecta a los ciudadanos y los textos que lo respaldan siendo protagonista las novedades europeas, podemos extraer las siguientes conclusiones:

1. La protección de datos de carácter personal es un derecho fundamental que varía según las fuentes jurídicas que estén en aplicación. Estas fuentes son el mero reflejo de lo que como sociedad vamos necesitando a medida que van surgiendo realidades como las tecnologías. La normativa recogida en la LOPD no ofrecía una protección al hilo de cómo estructuramos hoy en día nuestros datos, siendo un escenario principal Internet y las redes sociales.

2. El RGPD nace para dar respuesta a un mundo donde las fronteras físicas ya no tienen cabida, pues tanto la digitalización de nuestros datos como los verdaderos fines para los que los mismos se destinan, muchas veces quedan fuera del alcance del conocimiento que como ciudadanos tenemos de esta realidad. Todos y todas creemos que entrar a una red social significa única y exclusivamente una actividad de ocio sin un trasfondo que es real, donde los menores acceden sin ningún filtro a ellas, donde se comercializa con nuestros datos para después tener la posibilidad de crear perfiles de marketing que nos

terminan perjudicando. Poco a poco nos percatamos gracias a noticias mediáticas o a cuestiones que nos han afectado a nosotros directamente. Todo ello se ve reflejado en un RGPD mucho más restrictivo para las empresas, ofreciendo un control a los usuarios y usuarias, mucho mayor sobre sus datos personales. Lo cierto es que deberá adaptarse a cada caso concreto, a la casuística que añade aún más si cabe, desafíos jurídicos importantes. Las novedades más importantes en este sentido son:

A. El consentimiento que debe ser prestado de manera expresa, libre, consciente y darse ante unas condiciones vertebradas. Hay muchos lugares que manejan datos incluso con la categoría de sensibles, y que merecen el correcto tratamiento, el buen uso del consentimiento y la adecuación a todas las novedades que viene a traer el RGPD.
B. Quizá el ejemplo más claro a la novedad anterior hasta ahora ha sido el del derecho a no ser objeto de una decisión automatizada, pues muchas veces hemos intentado solucionar un problema y no hemos tenido la opción de hablar con una persona sino con un robot. Igual que hace 20 años no pensábamos en todo esto, ahora tampoco somos conscientes de lo que pasará en los próximos 20 años.
C. El llamado *Accountability* que precisa de un cumplimiento constante y de demostrarse que se cumple el RGPD.
D. La creación de la figura de DPD que sirve de enlace entre la empresa y el reglamento.
E. Sanciones Administrativas mucho más duras y adecuadas a los problemas que se dan en la práctica, en el mundo real.
F. La necesidad de comunicar las posibles vulneraciones a los datos de carácter personal a la autoridad de control que, como vimos, en España es la AEPD.

3. Personalmente considero que no existe una barrera de protección completamente adaptada a la realidad sobre la “venta” de los datos personales de todas las personas, pero aún así es importante darle el valor que se merece un salto tan cuantitativo como este, pues ya no importa dónde se traten los datos, sino que si son datos de personas europeas, el responsable que los

maneje deberá ceñirse al RGPD. Además, resaltamos que la gratuidad de las redes sociales que las hacen atractivas no es tal, pues pagamos un precio mucho más caro que el que se podría valorar en dinero puesto que el pago lo hacemos con nuestros datos personales, cuya protección no debemos olvidar que es un derecho fundamental.

4. Como dueños de nuestros datos personales que somos, debemos concienciarnos de los motivos que han impulsado los cambios que en este trabajo encontramos. Con ello deseo expresar que somos los que debemos invocar nuestros derechos siempre que consideremos que se han vulnerado, pero para ello primero es necesario hacernos conscientes de lo que valen nuestros datos. Es decir, las personas deben ser más conscientes de lo que supone tener una red social o navegar en Internet buscando unos contenidos u otros, atreverse a protestar cuando se hace algo que no se ha consentido con sus datos. Si como personas nos hacemos conocedores de todas estas cuestiones, será más fácil identificar los problemas como la lista *Robinson*, en la que al fin y al cabo debes inscribirte para que no se vulnere un derecho que de por sí es fundamental y que no precisa de ninguna inscripción a listas para que no se tenga en cuenta.

5. De la misma forma que el RGPD ha respondido a todas estas cuestiones, seguiremos evolucionando nosotros y nosotras hacia una manera diferente de concebir la comunicación y con ello seguirán evolucionando las formas en las que se guardan nuestros datos. El desafío jurídico que ello implica es de una importancia muy grande, ya que se crea una idea de desventaja permanente con la actualidad. De manera que siempre van a surgir nuevos mecanismos de recaudación de datos, diferentes formas de tratarlos, procesarlos y a su vez diferentes formas legales de darles protección, pero siempre condicionados a que primero se den los conflictos para luego ejercitar la protección que más se ajuste al caso concreto y a los casos en general. El RGPD con toda la novedad que presenta, necesitará un tiempo para observar cómo va acoplándose a la realidad, y será entonces cuando podamos afirmar si cubre completamente todas las necesidades que un derecho fundamental que hoy en día está tan quebrado, necesita.

VI. REFERENCIAS BIBLIOGRÁFICAS

9a Sesión Anual Abierta de la AEPD. Centro de Conferencias Fundación Pablo.

Agencia Española de protección de datos, *Informe 0197/2013*.

ÁLVAREZ, M. *Reglamento general de protección de datos: Hacia un nuevo modelo europeo*. Madrid 2016.

ARENAS, M. *El valor de la información personal: protección de datos personales y la sociedad del espectáculo*. Anuario de la Facultad de Derecho. Universidad de Alcalá, 2009, no.2. ISSN 1888-3214

ARENAS, M. *Integración Europea y protección de datos personales. Las garantías especificas del derecho a la protección de datos personales.* Anuario de la Facultad de Derecho Universidad de Alcalá, 2004-2005, vol. 2005. ISSN 1697-9699.

Article 29 data protection Working 2018.

BARRUISO, C. *Anuario de la Facultad de Derecho.* Universidad de Alcalá*,* 2009, no.2. ISSN 1888-3214.

BERROCAL, A. *Derecho de supresión de datos o derecho al olvido*. Madrid, 2017.

Blog de protección de datos. Disponible en: https://www.protecciondatos-lopd.com/empresas/normativa-detectives-privados/

BRAVO, A. *Utilidad y perjuicio en la red social*. Disponible en: http://www.revista-critica.com/la-revista/monografico/24-primeras-personas/37-utilidad-y-perjuicio-en-la-red-social

BUISÁN, N. *La ley de protección de datos. Análisis y comentario de su jurisprudencia.* En Carlos Lesmes Serrano. (coord.) 2008.

CHÉLIZ, MºC. *El "Derecho al olvido digital".* Universidad de Zaragoza*,* 2016.

COTERA, J.: *Relato del VII Congreso Internacional sobre Internet, Derecho y Política: Neutralidad de la red y derecho al olvido*, *IDP. Revista de Internet, Derecho y Política*, núm. 13, 2012.

COTINO, L. "*Big Data e inteligencia artificial*", Una aproximación a su tratamiento jurídico desde los derechos fundamentales, Dilemata, 2017.

DÍAZ, A. Origen y evolución de las redes sociales. Disponible en: http://socialmedialideres.com.ve/origen-y-evolucion-de-las-redes-sociales/

DPO&It Law. Disponible en: http://www.dpoitlaw.com/reglamento-general-de-proteccion-de-datos-rgpd-derecho-de-portabilidad-oposicion-y-a-limitar-las-decisiones/.

Entrevista Ángel Benito Roderó, 16 de abril de 2018, 09:00 h “Hub” Salamanca.

ESCRIBANO, P*. Los derechos a la intimidad y a la privacidad en el siglo XXI*. Madrid 2015.

FERNÁNDEZ, E., RGPD: *Seguridad, privacidad y oportunidad de negocio, Redseguridad* núm. 78, 2017.

FERNÁNDEZ, L. *El nuevo Reglamento Europeo de Protección de datos. Foro, Nueva época,* vol. 19, núm. 1, 2016.

GARCÍA HERRERO, J, *Reglamento Europeo de Protección de Datos: Guía Resumen*, 2017 disponible en: http://jorgegarciaherrero.com/reglamento-europeo-de-proteccion-de-datos-breve-guia-de-uso/

GARRIGA DOMÍNGUEZ, A., *Nuevos retos para la protección de datos personales en la Era del Big Data,* Dykinson, Madrid, 2016.

GIL, E. Big Data*, privacidad y protección de datos.* Agencia española de protección de datos Madrid, 2016.

GIL, E. *Cuando al robot no le gusta tu barrio*, Cuestiones del Big Data. *Blog Legal Today*. 2017.

GONZÁLEZ M. Disponible en: https://www.xataka.com/legislacion-y-derechos/que-ha-pasado-con-facebook-del-caso-cambridge-analytica-al-resto-de-polemicas-mas-recientes

HEREDIA, N. *Publicación de sentencias: Protección de datos vs interés público*. Disponible en: http://www.legaltoday.com/practica

IAB SPAIN, *Asociación de la publicidad, el marketing y la comunicación digital en España.* Disponible en: https://iabspain.es/wp-content/uploads/principales-aspectos-del-anteproyecto-lopd-iab-spain-1.pdf

InfoCuria – Jurisprudencia del Tribunal de Justicia. Sentencia del Tribunal de Justicia (Gran Sala) de 6 de octubre de 2015. Disponible en: http://curia.europa.eu/juris/document/document.jsf?docid=169195&doclang=ES

MORALES MARTÍN, T. *Funciones del nuevo Comité Europeo de Protección de Datos* 2017 disponible en: https://www.prodat.es/blog/funciones-nuevo-comite-europeo-proteccion-datos-parte-ii.html

MUNDO LOPD, *Infracciones y sanciones en el RGPD,* 2018. Disponible en: http://www.mundolopd.com/lopd/infografia-infracciones-sanciones-reglamento-general-proteccion-datos/

MUÑÓZ BARRIOS, A. *Tipos de decretos en España: Real Decreto, Real Decreto Legislativo y Real Decreto Ley.* Disponible en: http://queaprendemoshoy.com/tipos-de-decretos-en-espana-real-decreto-real-decreto-legislativo-y-real-decreto-ley/

NOAIN, A. La protección de la intimidad y la vida privada en internet*: La integridad contextual y los flujos de información en las redes sociales.* Agencia Española de Protección de datos, Madrid, 2015. p.168

PAGINA DE PRENSA Alto nivel. 16 de Mayo 2018. Disponible en: https://www.altonivel.com.mx/actualidad/internacional/dolor-de-cabeza-a-mark-zuckerberg/

PAGINA DE PRENSA La Vanguardia. *Instagram ofrecerá la posibilidad de descargar los datos compartidos.* 14 de Mayo 2018 Disponible en: http://www.lavanguardia.com/tecnologia/20180414/442488572158/instagram-privacidad-protecion-de-datos.html

PERIODICO DE NOTICIAS EL MUNDO. *Los marcapasos se pueden hackear*. 29 Mayo 2017. Disponible en: http://www.elmundo.es/tecnologia/2017/05/29/592be6a7268e3ecf4e8b4642.html

PERIODICO DE NOTICIAS El país. *Mar España: "Seremos beligerantes con todas las redes sociales*". 24 Mayo 2018. Disponible en: https://elpais.com/economia/2018/05/22/actualidad/1527003631_400767.html

PRIETO HERGUETA, J., *Guías y herramientas de apoyo para adaptarse al RGPD*. *Informática y salud* ISSN 1579-8070, núm. 127, 2018 p. 28-30

RALLO, A. *Protección de datos personales y redes sociales: obligaciones para los medios de comunicación*, Quaderns del cac, 2014.

Revista de prensa, *AEPD publica un sistema de notificación electrónica para comunicar la designación de Delegados de protección de datos*. Disponible en: https://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2018/notas_prensa/news/2018_04_10-ides-idphp.php

RICHTER, M. *Protección de datos de Carácter Personal como Derecho humano*. Revista Auctoritas Prudentium, Nº12, 2015.

SIMÓN, P. *El reconocimiento del derecho al olvido digital en España y la UE*. Barcelona 2015.

TRONCOSO, A. *Las redes sociales a la luz de la propuesta de reglamento general de protección de datos personales*. Revista Derecho, parte II, Universidad Oberta de Catalunya.

VIOLANTE, M. 5 cosas en las que se fijan los bancos al dar créditos. Disponible en: https://www.entrepreneur.com/article/268358

WATTS, D. *Seis grados de separación, la ciencia de las redes en la era del acceso*. Barcelona, 2006.

VII. Resumen en inglés

Throughout the human history, the way that we communicate has changed, since different languages to different supports such as stone, paper, etc. Messaging has become an essential tool to be in contact.

In the same way that Law was born in response to the most primitive conflicts, it also does it to the requirements required by changes, such as personal data protection regulation in terms of social networking.

Communication is a need and it has lead into multiple ways of conceiving. Social networking is another way to go and connect with others to the fact to share opinions, messages, thoughts, photos or even ‘likes’. In social networking, personal data integrated make possible all the working, data that deserve living up a protection.

Studying the news offered by GRDP to data protection is the purpose of this work. It becomes a legal source arranged to technological requests now.

That is to say, nowadays everybody uses Internet and social networking: that has reached to change the way of communication and all our data is commercialised indiscriminately without any direct knowledge.

Dating back social networking beginning, we must mention Randy Conrads who invented, in 1995, a web page in order to find some old classmates.

Due to the communication needs that we had referred to, Conrads’s page was an authentic success that other organizations used. Today, we can find some social networking considered the most used globally, as Facebook, Instagram or Twitter. It is important to say that an ideal of pleasant society and community is created which makes possible the success in social networking.

Moreover, they are presented as free, so it is more interesting. But, what users really pay is something that can not be quantified in money because it is more valuable, because they are our data.

Social networking and free searches online are paid by our data. These data, as we see then in this study, can turn against us for the possible creation of profiles for marketing purposes that can be discriminatory.

All conflicts that can appear in this field must be resolved by Law, who designated personal data protection right as a fundamental right.

It is so important to highlight that we are facing a fundamental right and it deserves therefore a special protection. A personal data is every that one makes recognizable a person, so activities performed in a social networking will be normally considered within this category. This is because, merely sharing a photo, user's data are making available in the social networking.

Nowadays, there are no effective procedures inside this networking to avoid that a minor can create a profile in, but law does to deal with this problem. At least with European citizens, protected by Regulation 2016/679 of the European Parliament and of the Council, of 27 April, on the protection of natural persons with regard to the processing of personal data and on the movement of such data.

In Spain, Regulation came into force on 2016. However, a period of 2 years for its application was allowed to all Member States with the aim of adapting properly.

Spain must finish developing the Organic Law concerning to this European Regulation, but until then, the Organic Law 1/1999, of 13 December, on personal data protection (OLDP) will be applicable, with the entry that will be applied in all that contradict the Regulation.

Personal data protection is extremely important because of data volume manipulated every day in enterprises, in schools, in hospitals, in administrative agencies, in associations, etc.

As a result of that, many enterprises have received cyberattacks in their personal computers or have just allowed not to implement a protection.

Personal data are more important than we think, because they can reach to determinate many aspects of our life by sharing with a high number of people.

A judgement from de National Audience of 15 June 2016 shows that: '*It shall be personal when processing data affect the private sphere of a person, their family and friend relationships, and the processing purpose shall take different effectiveness in these fields*'.

The structure of this work begins with the analysis of the Organic Law 15/1999. This is an Organic Law by the fact that it regularises a fundamental right, as it has already been remarked, regarding to the need we have in Article 81 CE concerning fundamental rights developed by an Organic Law

This law collects, among many important aspects, some topics as consent of the user, processing data, obligations of controller, etc.

Consent referred in this law is given by any person's wishes accepting the processing of his/her data. This consent must be appropriately informed before the person's permission in order to know the real purposes for his/her collected data.

In social networking, generally, a potential problem is posed: this consent is not appropriately given because users do not read privacy and data policy. In many cases, because of the large policy which is not presented appealing.

Information clear, expressed and unambiguous is specified even in OLDP. In practise, most people do not read this privacy and data policy. And that presents a problem because when the concerned person claims for damages, it will be impossible to claim something that has been given consent. As we will see later, that is a fact that European Regulation try to improve.

Another important question in consent is concerning the possibility of the exercise of the rights of access, rectification cancellation and object. That is to say, people have right to access to processing data, to cancelling and event to object them.

Finding information about a person in internet with a simple movement, nowadays it is easy. That is why this protection is needed.

New technologies must be a tool that facilitates people's life. And, in some cases, information that they have can damage their or just stop serving the purpose which consent was given.

In social networking, these rights must be effective within no more than 10 days by controller, who is the person responsible for processing data.

For a correct working, a number of principles are collected in OLDP -such as security or secret- and must be arranged to this specific case.

Responsible for filing must ensure this security and data protection avoiding that third party acquire it for different purposes not given in consent.

In this way, OLDP collect the right of compensation for people who suffer personal data's damages and injuries because of a bad working and bad protection completed by the controller.

Thus, controller's power is limited while user's powers of action is developed: that is the denomination received for all person who gives him or her consent.

European Regulation tries to resolve some problems that we had referred, for example, in case of consent where a consent order is required. It means that user has the possibility to object to some questions without losing his or her right to create an account in a social networking.
But, to immerse inside Regulation, first we need to indicate the field of application. Concerning protection, it is assumed very important because this regulation must be implemented to all people who process European citizen data.

Previously, any enterprise processing European citizen data's purpose was to argue not respecting the European normative because its head office could be registered outside of the European framework.

Today, that is not a problem because law must be implemented to anyone processing European citizen data, regardless of the place where they are processed.

To tackle all changes in the Regulation, I considered the expert opinion from Ángel Benito Roderó, who takes into consideration the following changes:

1. The right not to be subject to a decision based solely on automated processing.
2. The requirement of communicating security data breach to the supervisory authority.
3. The right to data portability.
4. Establishment of the European Data Protection Board.
5. Administrative penalties.

1. To follow an order, we start with the right not to be subject to a decision based solely on automated processing. This right is constituted for these users or interested who a robotic decision can have legal or similar effects. As we have already anticipated, we can be the object of a decision based on artificial intelligence guided by discriminatory patterns.

Banks have always used some data to grant loan banks. This activity has been extended until many enterprises use varied data to employ people possessing some profiles.

Big Data is characterized by administrating big flows of information: this information is extremely important to enterprises due to these reasons.
When a user is legally affected, Regulation collected this right that grants the communication with a person, not only with a machine.

In fact, the problem is that this right can be only exercised when user takes conscience about the ‘choice’ made by processing machine. This conscience is complicated in cases of work place’s choice.

2. On the other hand, the requirement of communicating ‘security data breach’ means that anyone processing personal data must communicate to the supervisory authority, in national case the Spanish Data Protection Agency (SDPA), the data (possible or not) infringement.

Controller of that processing must communicate it within 72 hours and to inform about the nature breach and their possible consequences.

This Regulation has a number of imperatives with a foresighted purpose in order to implement an action protocol to avoid these breaches before they were produced.

3. We also find a new right to data portability structured inside the right to be forgotten which authorise the applicant to take with him or her all data.

At this point it could be different conflict of interest, for example, between the freedom of expression concerning a subject and the right to be forgotten and data portability implicated.

4. The establishment of the European Data Protection Board who has legal personality. Its basic functions are supervising and granting the acomplishment of the regulation.

5. Substantial enough administrative penalties were introduced on it aimed to indemnify people suffering any processing data's damage not produced as provided by law.

These administrative penalties, in fact, will bring a huge quantity for big companies.

Another expert in this area, Jorge García Herrero, talks about the nuances introduced by Regulation concerning consent. This one must be granular, specific and freely given.

He explains us how consents given before the regulation, not accomplishing it, will not be valid any longer. In this sense, I explain how nobody should be included in a list so that their fundamental right on personal data protection were respected, and I mean to the Robinson list in which users are registered so that nobody calls them without their consent. Jorge García Herrero y Ángel Benito Roderó, they are both Data Protection Officers (DPO), a figure introduced by Regulation.

These DPO must advise processing controller about what they have to do, they also supervise normative compliance and explain to personnel the obligations attributed by regulation concerning data protection.

It can be DPO a lawyer, a jurist, a worker, etc. Its role consists in advice because enterprise, processing controller and workers, they decide, at the end.

Accountability is also important due to provide a requirement to enterprises for applying an active responsibility, verifying permanently the normative compliance, not only when problems appear.

Legitimate interest is also mentioned by Regulation. According to that, personal data can be processed rarely without person's consent.

This is reserved for situations of general interest or medical emergency in which data patient are necessary to save his or her life.

To conclude this work, I wanted to analyse in detail a specific case, such as social networking Instagram, reading its data privacy policy and seeing what aspects are not already implemented according to Regulation.

I chose this social networking because it is one of most important. It was acquired by Facebook in 2013. On this year, its privacy policy was taken effect but not adapted to Regulation.

First, it contains necessary information concerning the consent. However, this information is presented not clearly, it is rather large. 'Cookies' section remarks that given consent means to allow receiving information by publicity advertisers to user's device.

This information about products will be based in Big Data which user has contributed searching certain products on Instagram, such as clothes or shoes.

With the new Regulation, the consent must be granular or structured, that is to say, to allow users can refuse publicity reception.

Furthermore, there is a section 'How we use your information' that remarks all collected information from users can be compiled in Unites States or another place where Instagram has subsidiary.

This will also disappear with European Regulation's implementation because, even if they were complied in another place, normative must be respected, more if European citizen data are processed.

In fact, in the same privacy policy, it is reminded that Spanish normative is different in many other countries in which users' information can be complied.

While reading, I realise there is no mention to DPO, entity obligatory for a networking like Instagram that process intensively and massively personal data. They must be named in order to advice Instagram according with Regulation.

Reading on, it is included a section where they express not to be responsible for data, but they try to do it. Neither, they do not be responsible for modified or revealed users' information. Logically that will be different when the European Regulation is implemented.

Although the Regulation begins on 25th May of this year 2018, Instagram has not already taken measures for that, as well as communicating security breaches in maximum deadline of 72 hours.

The right to data portability is not even in that policy. In fact, it is explained how a user can close its account, but Instagram reserves the right to store its data whatever the time. Through the comparison I make, it is indeed a new instrument that allows to download all the photos, videos and comments that a person has uploaded to Instagram social network.

Regarding the deep study of user' consent in Instagram, it is neither adequate for Regulation. As we have indicated, it is not granular or structured, so it is unlikely to assure that they have given it just knowing the social networking purpose.

Given consent by users should absolutely be informed specially regarding the commercial purpose of data. So, I consider that it is an excessive and not proportional use to what anyone expects from a playful network.

For these reasons, GRDP requires to establish a conscious consent, a vertebrate consent for all to be aware of purposes of data processing. Communicating to supervisory authority the security breaches is absolutely

necessary because every day there are cyber-attacks in companies, and the precious object are personal data.

It is still an unknown world, specially because we don’t know the measure in which companies can affect themselves.

In reality, given consent by users should be informed, specially the data commercial purpose. That is the reason I consider it is an excessive and disproportionate use compared with what it is expected in a ludic networking.

At the moment, Instagram do not have settled the consent so that users can oppose for certain questions. But it is clear that it will never present the consent as a way to user for opposing that its data could be sold in market, as a Big Data.

That is the reason why Instagram, and any other social networking, is free because personal data are commercialized, but apparently it is just a virtual space where people share their opinions, photos, videos, etc.

The real problem is the big global lack of awareness: nobody sees social networking like a Trojan horse.

Few people know the commercial purpose of its data, the importance of that and the consequences involved.

Nobody imagines that the preference in a social networking by cooking publications can give as a result that sector companies send him or her some information about their services, for example.

This problem is accentuated considering the little time social networking is used. We are in a point of lack of awareness in which everything is allowed, in which we have not quantified truly the consequences.

If we use our rights every time we need them, that can be the solution. In this way, these rights can take a different form according to new needs that will appear.

To exercise our rights is in our hands: so that others can know that they also have the same rights. This RGDP is only applied to European citizens and to the treatment that is done on their data, which means that any other citizen of the world should abide by the regulation of their country in this sense, and by the multiple transnational agreements existing on this matter.