Revista CESCO de Derecho de Consumo **Nº 21/2017**

http://www.revista.uclm.es/index.php/cesco **I. Estudios y Consultas**

RESPONSABILIDAD CIVIL DERIVADA DE LA VULNERACIÓN DE LOS DERECHOS DE LA PERSONALIDAD EN LA RED

Lorena Parra Membrilla

Ganadora de la Primera Edición del Premio Ilustre Colegio Notarial de Castilla-La Mancha a Trabajos de Fin de Grado en Derecho Privado

Máster de Acceso a la Abogacía

Universidad de Castilla-La Mancha

Resumen: En la actualidad las plataformas virtuales, y sobre todo las redes sociales han revolucionado las comunicaciones y el modo de vida de toda la humanidad. Está cambiando el significado de términos como el de intimidad o propia imagen, ya que para muchos las redes sociales e Internet se han convertido en un diario directo de todo lo que sucede en sus vidas, dando lugar en ocasiones a la violación sistemática de los derechos de la personalidad debido a un incorrecto tratamiento de datos personales propios y de terceros sin otorgar un consentimiento expreso, real, valido y conscientemente prestado. El presente trabajo define cual es el alcance de la responsabilidad de estos servicios en el caso de que se dañen los derechos de la personalidad, y enfatiza la eficacia que el cumplimiento de los deberes contractuales puede tener en la protección de los intereses de privacidad e imagen de terceros. Por lo tanto, se da respuesta a si en realidad se tiene derecho a saber y a decidir que nuestros datos personales e incluso nuestras fotografías se muestren públicamente y en qué contexto. Además, se estudia cómo afrontan las redes la protección de la privacidad de sus usuarios y hasta dónde puede llegar el consentimiento prestado cuando nos creamos un perfil, analizando en qué casos los servicios web o incluso el propio usuario podrían ser responsables tanto civil como penalmente por la vulneración de este tipo de derechos fundamentales.

Palabras clave: red social, Internet, derechos de la personalidad, derechos fundamentales, datos personales, consentimiento, responsabilidad civil.

Title: Legal liability derivative of the violation of the personality rights in the net

Abstract: Nowadays, virtual platforms, and specially social networks have evolved communications and the whole humanity lifestyle. The meaning of may words, as privacy or self-look, are changing due to for many people, social networks and Internet have become a diary of everything happening in their lifes, coming sometimes into systematic violation of the rights relating to the personality because of the wrong usage of the personal data, both one it self and third-party, without

acknowlegde allowing an explicit, real, valid and conciously. The present paper defines which is the responsability of these services when the rights relating to the personality are damaged, it also empasizes effectiveness of compliance of contractual rights may have the protection of the interests of privacy and image of third parties. Therefore, in this paper we will answer if we really have the right to know and to decide that our personal date and even our photographs are displayed publicly and in what context. Also, it is studied how network of privacy protection deal with the privacy of their users and as far as consent can be obtained when we create a profile, analyzing in which cases the services of the networks or the user could be responsible both civilly and criminally for the violation of this type of fundamental rights.

Keywords: Social Network, Internet, personality rights, fundamental rights, personal data, consent, civil liability.

1. Introducción

Tanto Internet como las redes sociales han revolucionado las comunicaciones y con ello el modo de vida de toda la humanidad. Está claro que esta afirmación se amplía con relación a las nuevas generaciones que nacieron junto a esta nueva tecnología y que su vida actualmente depende de ella, sobre todo por la aparición de la web 2.0, permitiendo que cualquiera pueda crear una serie de contenidos y estos ser conocidos por todo el mundo. Pero la creación de estas nuevas redes no solo trae consigo beneficios, sino que también crea enormes problemas y sobretodo permanentes discusiones. El mayor problema de la inseguridad virtual lo genera el propio usuario que utiliza estos servicios virtuales, ya que es quien selecciona y coloca la información, muchas veces sensible, en manos de sitios que desconoce, y quien también acepta condiciones de contratación online sin leer, y muchas veces sin comprender, sus detalles.

Este trabajo intenta definir cuál es el alcance de la responsabilidad de estos servicios en el caso de que se dañen los derechos de la personalidad, y enfatiza la eficacia que el cumplimiento de los deberes contractuales puede tener en la protección de los intereses de privacidad e imagen de terceros. Por lo tanto, se

intentará dar respuesta a si en realidad se tiene derecho a saber y a decidir que nuestros datos personales e incluso nuestras fotografías se muestren públicamente y en qué contexto. Para ello, este trabajo estudiará cómo afrontan las redes la protección de la privacidad de sus usuarios, partiendo del momento en el que surgió esta personalidad virtual y hasta dónde puede llegar el consentimiento válido y eficaz cuando nos creamos un perfil en una red social e Internet, continuando con la normativa vigente y doctrina vinculante respecto a esta materia. Finalizaremos analizando en qué casos los servicios de la redes o incluso el usuario, podrían ser responsables tanto civilmente como penalmente por la vulneración de este tipo de derechos fundamentales.

Se trata de un tema complejo, ya no sólo en materia de conceptualización, sino debido a su constante cambio y por su escasa jurisprudencia, lo que me ha supuesto dificultades a la hora de su elaboración. Además de las sentencias analizadas, también se ha recurrido a la bibliografía disponible en la Universidad de Castilla-La Mancha, y a diversas páginas web jurídicas y base de datos de Aranzadi.

La metodología llevada a cabo en la realización de este trabajo se centra en las siguientes etapas:

- Primera etapa: Búsqueda de la bibliografía relacionada con la materia para su posterior análisis que me otorgue un conocimiento inicial sobre el tema.
- Segunda etapa: Creación de un índice, el cual se fue modificando y estructurando a lo largo de la elaboración del trabajo.
- Tercera etapa: Búsqueda y análisis de la jurisprudencia y de los diversos artículos y publicaciones jurídicas.
- Cuarta etapa: Redacción del trabajo a través de un análisis crítico y objetivo.

Para que se pueda realizar un análisis eficaz sobre el tema que permita comprender y sintetizar su amplitud y complejidad, se ha considerado oportuno que los tres primeros apartados del tema sean: el primero, dedicado al surgimiento de esta personalidad virtual y su conceptualización, el segundo, dirigido a un marco normativo global, y el tercero, conocer los derechos y deberes que entran en conflicto. Por otro lado, se tratara el consentimiento en materia de redes sociales e Internet, se continuará con el derecho al olvido y en último lugar se tratará la responsabilidad derivada de la lesión se los mismos. Para finalizar, se expondrán los aspectos más relevantes y a las conclusiones a las que se ha llegado con el estudio e investigación realizada.

2. El surgimiento de la personalidad virtual y su conceptualización

Tras la Segunda Guerra Mundial el mundo sufre una precaria situación, y debido al desarrollo del armamento nuclear culmina con el inicio de un nuevo conflicto, llamado la Guerra Fría. A pesar de no llegar a constituirse como un conflicto bélico, las tensiones producidas entre Estados Unidos y la Unión Soviética dividieron el mundo en dos bloques de países contrapuestos que se enfrentaban para implantar sus modelos de gobierno de manera global. Pero desde un punto de vista ideológico, la Guerra Fría significó la contraposición de dos teorías fundamentales,

por un lado la capitalista (sostenida por EE.UU y los países de la OTAN) y por otro lado, la comunista (sostenida por la Unión Soviética y los países aliados a ella). Esto tuvo una serie de consecuencias directas en la investigación y desarrollo de nuevas tecnologías. Es en el marco de la competencia entre ambas superpotencias, donde se hallan los inicios de la informática moderna.

En 1957 la Unión Soviética lanzó y puso en órbita el primer satélite artificial "Sputnik", lo que significó el inicio de la carrera espacial. Debido a estos logros, el gobierno estadounidense dio inicio en 1958 con su Agencia de Proyectos de Investigación Avanzada uno de sus proyectos, el llamado ARPANET, el cual es, según MORALES VIALES y UGARTE IBARRA, "un proyecto que desarrollaría la creación de una red de comunicación entre ordenadores. La particularidad de la iniciativa radicaba en la descentralización del sistema".[1]

A raíz de esto, ARPANET se convirtió en el internet, en una red global que se basaba en la idea de que "existirían múltiples redes independientes de diseño arbitrario, iniciando con la ARPANET como la red pionera"[2], lo que dio lugar a la aparición del transistor (1958), el nacimiento del "miniordenador" en el año 1965, y el desarrollo de los actuales sistemas computacionales en paralelo a partir de 1990[3].

Esta evolución culminó con el surgimiento de la actual "sociedad de la información", en la cual las tecnologías que facilitan la "creación, distribución y manipulación de la información que juegan un papel esencial en las actividades sociales, culturales y económicas"[4]. Éstas conducen al individuo a la utilización de las tecnologías para la realización de actividades diarias, para lo que este individuo debe adoptar una presencia virtual.

Esta personalidad virtual representa según CHINCHILLA SANDÍ, "el desdoblamiento del ser humano en su materialidad física y su desmaterialización virtual de información (principio de ubicuidad), donde esta personalidad virtual conformada en forma absoluta de información se encuentra regulada por cada persona y será considerada como centro de atribución o imputación de efectos jurídicos"[5]. Por lo tanto, lo entenderíamos como una manifestación virtual de la personalidad individual.

La expresión "red social" como tal fue propuesta por JOHN BARNES antropólogo británico, en 1954, en un estudio de campo que el mismo realizó sobre la

[1] MORALES VIALES, R; Y UGARTE IBARRA, R*: Tutela de los derechos de la personalidad virtual y protección de datos de carácter personal en las redes sociales online*, Instituto de Investigaciones Jurídicas de la Universidad de Costa Rica, 2012, p.11.

[2] LEINER, B; CERF, V; CLARK, D; KAHN, R; KLEINROCK, L; LYNCH, D; WOLFF, S*: A brief history of the Internet*, Universidad de California, Santa Bárbara, 2009, p. 24.

[3] MORALES VIALES, R Y URGATE IBARRA, R: *Tutela de los derechos…*, ob.cit., p.13.

[4] CARRIÓN, H: *La sociedad de la información. Tecnologías de información y telecomunicaciones*, Centro de Investigación para la Sociedad de la Información, 2013, p. 86.

[5] CHINCHILLA SANDÍ, C: "Personalidad virtual: necesidad de una reforma constitucional", en *Revista de Derecho y Tecnologías de la información*, 2005, p. 5.

comunidad rural, pero, si es cierto, que el funcionamiento de las redes sociales fue planteada en el año 1929 por FRIGYES KARINTHY (escritor húngaro) en su relato llamado "Chains". Fue desde entonces cuando se comenzó a estudiar el fenómeno por diversas disciplinas, proponiendo así diversas teorías, como fue la famosa "Seis Grados de Separación", propuesta por DUNCAN WATTS, basada en el planteamiento de KARINTHY, la cual sostiene según ISABEL PONCE, "que se puede acceder a cualquier persona del planeta en sólo seis saltos, por medio de una cadena de conocidos las personas están relacionadas unas con otras a través de cinco intermediaros. Se basa en la idea de que el grupo de conocidos crece exponencialmente con los enlaces en cadena, y harían falta, únicamente, cinco de estos enlaces para cubrir la totalidad de la población mundial […] El software original de las redes sociales virtuales parte de esta teoría, de hecho existe en EE.UU una patente llamada six degrees patent por la que ya han pagado las redes sociales Linkedin y Tribe"[6].

Como bien afirma CEREZO[7], estamos ante un cambio de paradigma desde la aparición de internet, y sobre todo con la llegada de la web 2.0[8]. La Red es un nuevo espacio donde los roles de los diferentes usuarios se construyen, evolucionan y cambian. Es un área donde los intermediarios tradicionales han perdido toda credibilidad y han surgido nuevos influyentes vinculados con las redes sociales, lo que ha dado lugar a nuevas formas de organización y relación.

El Instituto Nacional de Ciberseguridad, señala que "Internet ha creado un nuevo escenario en el que las relaciones personales cobran protagonismo […] Nuevas plataformas y herramientas colaborativas, produciendo un cambio desde una Web 1.0 basada en páginas estáticas e informativas, sin capacidad de generar una participación del usuario, hacia una Web dinámica donde se produce una interrelación que genera una suma de conocimientos y/o experiencias, es decir, la Web 2.0 (o Web social). Son personas colaborando, compartiendo y participando en un canal multidireccional abierto que permite lograr la máxima interacción entre los usuarios y les ofrece nuevas posibilidades de colaboración, expresión y participación"[9].

Por lo tanto, a diferencia de la Web 1.0, que solo era de lectura, la Web 2.0, es de lectura y escritura, donde se tiene la posibilidad de compartir información constantemente. Esta es llamada la Web social, ya que está integrada por medios de comunicación sociales, denominados Medios sociales o Social Media, que a diferencia de los Mass Media, en este caso el usuario pasa de ser consumidor de la Web, a interactuar con ella y con los demás usuarios de diversas formas.

---

[6] PONCE, I: *Redes Sociales*, Instituto de Tecnologías de la Comunicación, 2012, p. 1.

[7]CEREZO GILARRANZ, J: "Presentación. Identidad digital y reputación online", en *Cuadernos de comunicación Evoca. Evoca Comunicación e Imagen,* 2011, p. 5.

[8] Nuevos sitios web que se diferencian de los sitios web más tradicionales llamados Web 1.0.

[9] PEREZ, P; GUTIERREZ, C; DE LA FUENTE, S; GARCÍA, L; ALVAREZ, E: *Guía de Introducción a la Web 2.0: aspectos de privacidad y seguridad en las plataformas colaborativas*. Instituto Nacional de Tecnologías de la Comunicación, 2011, p.4.

Actualmente, el acceso a las redes sociales a través de Internet se amplía con nuevos medios como son los "smartphones"[10], que permite la conexión en cualquier momento, y también en cualquier lugar.

Existen servicios de redes sociales de todos los tipos, y son utilizados por las diversas generaciones para diferentes finalidades, llegando a crear nuevas oportunidades de negocio, pero también ciertos riesgos para la privacidad.

Ya en 2007, la ENISA (European Network and Information Security Agency) publicó "Security issues and Recommendations for on line social networks", donde se estipulaban los principales desafíos en las redes sociales y recomendaciones. Además en 2008, el IWGDPT (International Working Group on Data Protection and Telecomunications) aprobó el "Rome Memorandum" en el que se analizaban los riesgos para la privacidad y seguridad de las redes sociales e Internet[11]. Estas reuniones van dirigidas a todos los usuarios participantes de las redes sociales, pero en especial a los denominados "nativos digitales", que eran aquellos que habían nacido y crecido en el entorno de la tecnología y que, teniendo otro concepto de privacidad, se sienten cómodos publicando detalles de sus vidas en la red.

Por todo esto, en 2009, se aprobó un Dictamen (5/2009) por el Grupo de Trabajo del Grupo Europeo de Protección de Datos, sobre redes sociales online en el que se analiza el cumplimiento de éstas ante la legislación de la UE en materia de protección de datos, concretamente sobre los roles y responsabilidad de los actores en estas plataformas.

3. Marco normativo en materia de protección de datos personales

3.1 Marco internacional

En la actualidad resulta imposible identificar un marco de Derecho Internacional aplicable a todos los países del mundo. Nos encontramos en un momento histórico difícil para la protección universal de los datos de carácter personal.

A pesar de esto, podemos encontrar ejemplos de sistemas internacionales que intentan otorgar bases legales que den la posibilidad del ejercicio del derecho fundamental a la autodeterminación informativa de manera internacional[12]. Por lo que, existen algunos sistemas que han surgido a partir de los modelos regionales y que se han extendido en la esfera internacional para poder admitir situaciones especiales o para reconocer

[10] Los "smartphones" son los actuales teléfonos móviles, los cuales permiten a los usuarios conectarse a internet, gestionar los servicios red, instalar aplicaciones u otros recursos al igual que en un ordenador.

[11] Es importante resaltar que la aprobación por este Grupo de la "Carta de derechos de privacidad en el mundo digital", también conocida como "Declaración de Granada", impone a los usuarios el deber de ser singularmente diligentes a la hora de evitar suministrar información no autorizada.

[12] SUÑE, E: *Del derecho informático al derecho del ciberespacio y a la constitución del ciberespacio*. Iuris Tantum vLex, 2006, pp. 318-319.

su interoperabilidad con otros marcos normativos, como es el programa "Safe Harbor"[13] aplicado en EE.UU[14], así como el reconocimiento de una protección adecuada en otros países.

Por otro lado, existen algunos sistemas establecidos por entes internacionales que intentan establecer las bases para la futura construcción de un modelo normativo internacional estable como son: APEC, Naciones Unidas y OCDE.

3.1.1 Modelo estadounidense

Es importante mencionar este modelo, ya que la mayoría de servidores de las redes sociales y de internet, tienen su sede principal en este territorio.

El sistema legal de Estados Unidos, basado en el "common law"[15], tiene una percepción distinta en materia de privacidad de la existente en el resto de países. Estas diferencias, unidas con los ideales liberales por los que se caracteriza el gobierno estadounidense han generado en este país un sistema totalmente opuesto al sistema europeo, en el que se ha evitado la regulación gubernamental de las políticas de privacidad y protección de datos, y se ha optado por fomentar un modelo de regulación mínima[16]. Según KIRSH, PHILIPS Y MCINTYRE, "pese a que los norteamericanos son agudamente sensibles sobre su privacidad en el ciberespacio, también son reacios a empoderar al gobierno para que proteja su privacidad […] La demanda del consumidor debería guiar a los proveedores hacia la promoción de sus medidas de protección a la privacidad en su esfuerzo por acumular una mayor cuota de mercado sobre aquellos competidores que no ofrezcan medidas similares"[17]. Por lo tanto, como mencionan estos autores, el sistema de regulación mínima deja a disposición de las empresas y de los consumidores la toma de decisiones en esta materia, infiriendo únicamente el estado donde sea necesario. Pero, a pesar de esta situación, el marco legislativo actual cuenta con una gran cantidad de legislación (aunque

[13] El programa "Safe Harbor", fue creado en 1990 para dar respuesta a la difícil realidad que resultó para EE.UU la adopción de la Unión Europea de la Directiva 95/46/CE en materia de protección de datos, aplicando en este programa algunos de los principios de la Directiva. Se constituyó con la idea de que aquellos datos personales y sensibles procedentes de Europa que quieran ser almacenados en EE.UU o viceversa, deberán contar con la misma protección de que gozan en el continente del que son recopilados.

[14] QUESADA, A: *Protección de datos y telecomunicaciones convergentes,* Agencia Española de Protección de Datos, Madrid, 2015, pp. 362-365.

[15] Consiste en el derecho común vigente en la mayoría de los países anglosajones. Es un sistema legal basado en las decisiones adoptadas por los tribunales, en contraste con los sistemas de Derecho civil.

[16] GUADAMUZ, A: "Habeas Data: The Latin American Response to Data Protection. Warwick website", en *Electronic Law Journals,* 2000, p.1.

[17] KIRSH, E; PHILIPS, D; MCINTYRE, D: "Recommendations for the Evolution of Cyberlaw*"*, en *Journal of Computer-Mediated Communication*, Indiana, 1996, p.1.

sea de regulación mínima) y jurisprudencia relacionada con la protección de la privacidad.

3.2 Marco europeo

Europa posee en la actualidad el sistema más completo y complejo de protección de datos personales a nivel mundial, y se constituye como referente obligatorio de regulación de la materia y como único ejemplo funcional del sistema internacional de protección de datos. Fundado en las declaraciones internacionales de derechos humanos y los tratados constitutivos de la Unión Europea, éste procura conseguir la protección de los datos personales a raíz del establecimiento de una serie de directivas y regulaciones dirigidas a los estados miembros y que establecen pautas mínimas de protección aplicables entre ellos.

3.2.1 Marco legal fundamental

En primer lugar, y como apertura de este marco legal fundamental, se encuentra la Carta de los Derechos Fundamentales de la Unión Europea[18]. Fue declarada el 7 de diciembre del 2000, pero no se dieron sus efectos hasta la entrada del Tratado de Lisboa en el 2009 (paso fundamental para la unificación normativa de los Estados Miembros). Ésta consagra derechos políticos, sociales y económicos para los ciudadanos y residentes de la Unión Europea. Posee carácter vinculante para toda la corte que aplique el marco normativo europeo, y particularidad de considerar su art. 8 a la protección de datos personales como un derecho fundamental, pudiendo cualquier persona exigir que todo tratamiento de sus datos personales sea realizado "de modo leal, para fines concretos y sobre la base del conocimiento de la persona afectada […]. Derecho de toda persona a acceder a los datos recogidos que la conciernan y a su rectificación […] estando sujeta al control de una autoridad independiente".

Por otro lado, también se encuentra, el Tratado de la Unión europea[19]. Éste fue firmado el 7 de febrero de 1992 y se encarga de dirigir el funcionamiento de la Unión. En materia de protección de datos personales, el Tratado adquiere importancia al establecer disposiciones relevantes en su art. 6, comprometiendo a todos sus países miembros a adoptar el marco jurídico europeo sobre derechos fundamentales y especificar el estatus jurídico que deberán poseer dentro del sistema legal Europeo, brindando así seguridad jurídica a los sujetos en materia de tratamiento de datos personales a lo largo de la Unión y la posibilidad de protección de forma coordinada con el ámbito regional en esta materia. Y también en su art. 39, que permite coordinar

[18] DOUE, núm.364, de 18 de diciembre de 2000 (2000/C 364/01).

[19] DOUE, núm.340, de 10 de noviembre de 1997 y BOE, de 13 de enero de 1994.

políticas conjuntas en materia de seguridad que nivelen y dirijan dichos esfuerzos en la materia.

De igual forma tenemos el Tratado sobre el Funcionamiento de la Unión Europea[20]. Fue firmado en Roma en 1952 y es uno de los textos más antiguos, siendo reformado en diversas ocasiones. Éste detalla las diversas políticas y acciones que definirán a la Unión, establecimiento los principios constitucionales y jurídicos que rigen todos los ámbitos de esta. En el contexto de protección de datos personales el Tratado lo refleja en las disposiciones de su art. 16, las cuales garantizan un lugar privilegiado a la protección de datos a la vez que eleva el conocimiento de la protección al nivel del Parlamento Europeo y el Consejo de Europa, lo que ha dado lugar a la formación de diversas Directivas.

Finalmente, se encuentra el Convenio 108 del Consejo de Europa del 28 de enero de 1981[21], para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal. Fue firmado en Estrasburgo el 28 de enero de 1981 por un comité de expertos gubernamentales bajo la autoridad del Comité Europeo para la cooperación legal. Es actualmente el único instrumento internacional jurídicamente vinculante para ser aplicado globalmente. Éste procura reforzar la protección de datos mediante una serie de principios fundamentales reconocidos universalmente, a la vez que establece normas jurídicamente vinculantes y disposiciones neutras capaces de adaptarse a los diversos marcos legales internacionales, tanto para el ámbito público como el privado. Requiere de los Estados firmantes su aplicación a los ficheros y tratamiento automatizados de datos de carácter personal que se realicen por los ámbitos públicos y privados, a la vez que requiere que se adopten principios para su protección como los de tratamiento justo y legal, la adecuación al fin del tratamiento, la relevancia y no exceso de los datos obtenidos, y la limitación del tiempo de estos.

De este Convenio, se despliega el Protocolo adicional al Convenio 108 del Consejo de Europa[22], para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, a las autoridades de control y a los flujos transfronterizos de datos. Éste procura mejorar la aplicación de los principios del Convenio anteriormente comentado, por medio de la inclusión de provisiones vinculantes necesarias frente al intercambio de los datos personales causado por la globalización y el progreso. Crea autoridades supervisoras, como entes investigativos y de intervención, capaces de incoar procesos judiciales y regula con mayor detenimiento los flujos transfronterizos de datos personales a países no miembros.

[20] DOUE, núm. 83, de 30 de marzo de 2010 (Versión consolidada).

[21] BOE, núm. 274, de 15 de noviembre de 1985.

[22] De 8 de noviembre de 2001.

3.2.2 Directivas

En primer lugar, se encuentra la Directiva 2002/58/CE, del Parlamento Europeo y del Consejo de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas[23]. Esta Directiva actualizó la Directiva 97/66/CE en materias de privacidad y comunicaciones electrónicas. Constituyó provisiones decisivas para la creación de confianza por parte del usuario en los servicios que se prestaban en las tecnologías de la información y comunicación. Además establece los fundamentos para el procesamiento de datos en los servicios de comunicación con disposiciones relativas a: seguridad en el procesamiento, retenciones de datos, comunicaciones no solicitadas (aquel correo no deseado o como se denomina actualmente "spam"), las cookies, los directorios públicos y el establecimiento de controles gubernamentales.

No obstante, esta Directiva de 2002, es modificada por la Directiva 2009/136/CE, la cual es adoptada por el Parlamento Europeo y el Concejo de la Unión Europea el 25 de noviembre de 2009[24]. Se centra en el reforzamiento de las disposiciones ya existentes en materia de consentimiento, y sobre todo para la instalación de cookies en los dispositivos de los usuarios. Ésta, considera el consentimiento informado esencial para determinar la capacidad de una página para la instalación de cookies. Además establece la capacidad de las autoridades nacionales competentes de dictar directrices frente a una vulneración de los datos personales y de realizar autorías para su cumplimiento.

Por otro lado, también encontramos la Directiva 2016/680 del Parlamento Europeo y del Consejo, 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y la libre circulación de dichos datos[25], la cual, deroga la Decisión Marco 2008/977/JHA del Consejo. Está directamente destinada a los ámbitos policiales y de justicia, asegurando que los datos de las víctimas, testigos y sospechosos de la perpetración de un delito se encuentren protegidos en el ámbito de la investigación criminal. Además facilita la cooperación transfronteriza de la policía y los órganos jurisdiccionales.

[23] DOUE, núm. 201, de 31 de julio de 2002.

[24] DOUE, núm. 337, de 18 de diciembre de 2009.

[25] DOUE, núm. 119, de 4 de mayo de 2016.

3.2.3 Reglamentos

Resulta inevitable mencionar el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos[26], y por el que se deroga la Directiva 95/46/CE. La Directiva 95/46/CE era del año 1995, cuando ni siquiera existía cloud computing[27] o Facebook, y además cuando un porcentaje minoritario de personas usaba internet, lo que ha provocado que esta directiva en gran medida quedara obsoleta. Facebook supuso una revolución de igual magnitud que en la que su día provocó GUTENBERG con la invención de la imprenta, con la diferencia del factor tiempo, ya que MARCK ZUCKERBERG, el creador de Facebook tardó 5 años en llegar a miles de millones de personas en todo el mundo, mientras que GUTENBERG tardó 3 siglos en llegar a ese número de personas[28]. Debido al desfase ambiguo de la Directiva, se creó este nuevo reglamento, el cual modernizó y unificó la normativa Europea sobre la protección de datos, permitiendo así a los ciudadanos un mejor control de sus datos y a las empresas poder aprovechar las oportunidades del mercado digital, reduciendo por un lado la burocracia y beneficiándose por otro, de una mayor confianza de los consumidores.

Este Reglamento es destinado al tratamiento total o parcialmente automatizado de los datos personales, y al tratamiento no automatizado de los datos personales contenidos o destinados a ser incluidos en un fichero, y será de aplicación en cada Estado Miembro y obligatorio en todos sus elementos. Además pretende consolidar los criterios comunitarios en materia de imposición de sanciones, así como de aumentar su cuantía para garantizar una mayor protección. Por lo tanto, amplía el alcance de sus sanciones hacia los responsables del tratamiento que no se ciñan a la normativa, y autoriza a las autoridades nacionales de esta materia (como es la AEPD) a imponer sanciones administrativas, pudiendo los interesados presentar reclamación frente a estas, así como su derecho a la tutela judicial de los mismos ante los órganos jurisdiccionales de cualquier Estado Miembro. Según su art. 99: "entrará en vigor a los veinte días de su publicación en el Diario Oficial de la Unión Europea", pero solamente será aplicable a "a partir del 25 de mayo de 2018".

3.3 Marco nacional español

El sistema normativo Español se enmarca dentro de la aplicación del sistema normativo Europeo de protección de datos personales. En España,

[26] DOUE, núm. 119, de 4 de mayo de 2016.

[27] Es un modelo que ofrece servicios de computación a través de Internet, es decir, ofrece al usuario el acceso a un conjunto de prestaciones o servicios estandarizados. Es también denominado la Nube.

[28] TESONE, R: "Los retos de la privacidad: innovación, derecho y seguridad", en *CEU*, Madrid, 2014, p.1.

el marco normativo en materia de protección de datos de carácter personal se basa, principalmente, en el reconocimiento constitucional de la intimidad personal, el secreto de las comunicaciones y la protección de los datos personales del art. 18 de la CE.

Pero, también encontramos la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD)[29], que va dirigida a armonizar este sistema con la Directiva Europea de Protección de Datos personales. Según esta, se pretende "garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar".

Esta normativa establece los derechos que son de aplicación para el sujeto sometido al tratamiento de los datos personales, como puede ser: tener conocimiento de que sus datos están siendo utilizados, ya sea por el sector público o privado, poder acceder en cualquier momento, corregirlos, incluso solicitar su destrucción. También contempla disposiciones en materia de seguridad de datos, deber de secreto, acceso a los mismos por cuenta de terceros y derecho a indemnización, además de unas reglas más específicas para ficheros de titularidad pública y privada.

Respecto al movimiento internacional de los datos personales, tiene como regla general esta Ley: "que no podrán realizarse trasferencias temporales ni definitivas de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento con destino a países que no proporcionen un nivel de protección equiparable al que presta la presente Ley". Además establece en su art. 35, como ente encargado de decidir sobre el nivel de protección a la Agencia de Protección de Datos.

La Ley Orgánica 15/1999 ha sido complementada y fortalecida por diversos decretos reales, encontramos entre ellos: el Real Decreto 1720/2007[30], que complementa a la LOPD en materia de consentimiento de menores de edad y medidas de seguridad en bases de datos manuales, procedimientos administrativos relaciones y transferencias internacionales de datos; Real Decreto 3/2010[31], que pretende evitar el intercambio de datos sin el consentimiento del usuario de ese tratamiento.

Sería interesante nombrar también la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen[32], ya que es parte fundamental de nuestro trabajo por su vulneración en el tratamiento de los datos personales. Ésta Ley

[29] BOE, núm. 298, de 14 de diciembre de 1999.

[30] BOE, núm. 17, de 19 de enero de 2008.

[31] BOE, núm. 25, de 29 de enero de 2010.

[32] BOE, núm. 115, de 14 de mayo de 1982.

Orgánica tiene como finalidad la protección civil y garantía del art. 18.1 de la CE, relativo al derecho al honor, a la intimidad personal y familiar y a la propia imagen. Se regula en ella, por lo tanto, el ámbito de protección de estos derechos y se establece un cauce legal para su defensa en el supuesto de injerencia o intromisión ilegítima, o las demás pretensiones que podrá deducir el perjudicado.

4. Derechos y libertades en conflicto

En la Declaración Universal de Derechos Humanos de 1948[33] no aparecían el derecho al honor, a la intimidad personal y familiar y a la propia imagen, sino que está reflejaba textualmente "nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra ni a su reputación", ya que en este tipo de sociedades agrarias y con relaciones muy limitadas, no existía tal necesidad de protección. Fue con la aparición de la sociedad industrial y el desarrollo de las nuevas tecnologías, especialmente en materia de comunicaciones lo que hicieron que fuera más difícil conservar intacto el ámbito de la vida privada, por lo tanto, fue a raíz de la Constitución de 1978[34] cuando se empezaron a reconocer. Actualmente están reflejados en el art. 18.1 de la misma, que afirma lo siguiente "se garantiza el derecho al honor, a la intimidad personal y familia y a la propia imagen". El constituyente además estableció como previsión de posibles incidencias de estas nuevas tecnologías un último apartado en el art. 18 CE referido a este ámbito que se expresa así "la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".

a) El derecho al honor

El honor es un concepto jurídico indeterminado, versátil en función de las normas, valores e ideas sociales que estén vigentes en cada momento. Por lo que el derecho al honor, según el Tribunal Constitucional consiste "[…] en ese derecho que ampara la buena reputación de una persona, protegiéndola frente a expresiones o mensajes que lo hagan desmerecer en la consideración ajena de ir en su descrédito o menosprecio o que sean tenidas en el concepto público por afrentosas"[35]. El derecho al honor consiste, según la doctrina, en el derecho al respecto y al reconocimiento de la dignidad personal necesaria para el libre desarrollo de la persona en una convivencia social.

Por lo tanto, el derecho honor ampara la buena reputación de una persona, tanto a nivel subjetivo (según la estimación que se tenga cada persona de ella

[33] BOE, núm. 243, de 10 de octubre de 1979.

[34] BOE, núm. 311, de 29 de diciembre de 1978.

[35] STC (Sala 1ª) de 15 de enero 2007 (FJ 3), (RTC 2007, 9). En sentido parecido, vid. SSTC (Sala 1ª) de 11 de abril de 2011 (RTC 2011, 41) y de 23 de marzo de 2009 (RTC 2009, 77). Asimismo, las SSTS (Sala 1ª) de 5 de mayo de 2009 (RJ 2009, 147) y 7 de noviembre de 2008 (RJ 2008, 5903).

misma) como a nivel objetivo (según la consideración que se tenga por los demás de esa persona).

b) El derecho a la intimidad personal y familiar

El derecho a la intimidad como derecho fundamental protegible surgió ya en 1890 con el artículo "The Right to Privacy (derecho a la privacidad)" el cual señaló la doctrina constitucional, de SAMUEL D. WARREN y LUIS BRANDEIS, en el que configuraban a la privacidad como un derecho a la soledad ("el derecho a estar solo" o "el derecho a ser dejado tranquilo y en paz"[36]).

Este es un derecho vinculado con la dignidad de la persona, que según nuestro Tribunal Constitucional, implica la subsistencia de una esfera propia y reservada frente a la acción y el conocimiento de los demás, siendo necesario para tener una mínima calidad de vida humana[37]. Pero este derecho no implica únicamente la preservación de su esfera propia e íntima, si no la no revelación o divulgación de datos personales no consentidos, al igual que su uso y explotación, ya no solo del individuo en sí, si no como también nombra el artículo, de su familia.

c) El derecho a la propia imagen

Este derecho garantiza, según el Tribunal Constitucional, el ámbito de libertad de una persona respecto de los atributos más característicos, propios e inmediatos, como por ejemplo es la imagen física (figura humana visible), el nombre o la voz[38].

Es un derecho autónomo, aunque está íntimamente relacionado con el derecho al honor, y de forma especial con el derecho a la intimidad, ya que lo que se pretende con ellos es proteger un espacio de intimidad personal y familiar sustraído de intromisiones extrañas.

El derecho a la propia imagen comporta una vertiente constitucional, pero también otra patrimonial, ya que por medio del consentimiento del titular, la imagen puede convertirse en un valor autónomo de contenido patrimonial, es decir, sujeto al tráfico comercial. Es este el momento en el que el derecho pierde su vertiente constitucional y por lo tanto su protección como derecho fundamental y éste solo estará sujeto a las normas de derecho civil, mercantil o laboral. En este sentido el Tribunal Constitucional lo afirma así: "la protección constitucional de este derecho no alcanza su esfera patrimonial, ya que el conjunto de derechos relativos a la explotación comercial de la imagen

[36] LÓPEZ DÍAZ, E: *El derecho al honor y el derecho a la intimidad*, ed Dykinson, Madrid, 1996, p.175.

[37] STC (Sala 1ª) de 15 de noviembre de 2004 (FJ 2ª), (RTC 2004,196). Asimismo, vid. SSTC (Sala 1ª) de 23 de marzo de 2009 (RTC 2009, 70), de 24 de septiembre de 2007 (RTC 2007, 206), de 3 de julio de 2006 (RTC 2006, 196), de 30 de junio de 2003 (RTC 2003, 127), entre otras. También la STC (Pleno) de 9 de mayo de 2013 (RTC 2013, 115). Precisamente esta última se refiere a los límites de este derecho fundamental.

[38] STC (Sala 2ª) de 25 de abril de 1994 (FJ 3º), (RTC 1994,117).

no forman parte del contenido del derecho fundamental a la propia imagen que consagra el art. 18.1 CE, las posibles consecuencias patrimoniales del uso ilegítimo de la imagen ajena no obstan para su protección constitucional"[39].

Estos derechos de la personalidad tienen una serie de límites especiales los cuales son también derechos fundamentales y están recogidos por la constitución de 1978 en su art. 20. En el supuesto de conflicto entre los derechos de la personalidad y los recogidos en el art. 20 de CE, este será resuelto por medio de la ponderación constitucional, teniendo en cuenta el valor preferente del derecho y las circunstancias concreta de cada caso. Estos límites son:

- Libertad de expresión, que según el art. 20 CE: Es aquel derecho de poder expresar y difundir libremente pensamientos, ideas, opiniones o juicios de valor (inherente al principio de legitimidad democrática), ya sea mediante la palabra, de forma escrita o mediante cualquier otro medio[40].
- Libertad de información, que según el art. 20.1 CE: Es el derecho a recibir o comunicar libremente información veraz por cualquier medio de difusión. Pero, no es protegible cualquier información, solamente será aquella que sea veraz, relativa a asuntos de interés general o relevancia pública y corrección de formas (utilización de términos y expresiones adecuadas)[41]. Como complemento del derecho de información encontramos el derecho de rectificación, que a pesar de no estar mencionado en la Constitución, está regulado en España como si de un derecho fundamental se tratara aunque existe una gran discrepancia doctrinal en esta materia[42]. El derecho de rectificación consiste en "el reverso del derecho de información ejercido por los profesionales a través de medios de comunicación institucionalizados"[43], es decir, en la rectificación de informaciones publicadas por los medios, siendo esta solicitada por considerarse lesivas de derechos propios.

5. El consentimiento en las redes sociales e internet

El derecho a la protección de datos personales consiste, según lo establece el Tribunal Constitucional: *"en garantizar a la persona un poder de control sobre sus datos personales"*[44], es decir, en que el sujeto tenga la capacidad de disponer de sus datos personales[45]. Para que este control sea efectivo, el sujeto debe de disfrutar de una serie de facultades que conforman el contenido del derecho que,

[39] STC (Sala 1ª) de 27 de abril de 2010 (FJ 4º), (RTC 2010,23).

[40] Constitución Española de 1978 (BOE, núm. 311, de 29 de diciembre de 1978).

[41] STC (Sala 2ª) de 26 de enero de 2009 (FJ 4º), (RTC 2009, 29).

[42] LIZARRA VIZCARRA, I: *El derecho de rectificación*, ed Aranzadi. Cizur Menor, Navarra, 2005, p. 63.

[43] PEREZ ROYO, J: *Curso de Derecho Constitucional*, ed Marcial Pons, Madrid, 2010, p.346.

[44] STC (Pleno) de 30 de noviembre de 2000 (FJ 6º), (RTC 292, 2000).

[45] Como ya hizo la STJUE (Gran Sala) de 13 de mayo de 2014 (TJCE 2014, 85), la STS (Sala 3ª) de 15 de marzo de 2016 (RJ 2016, 1301), precisamente califica la actividad de motor de buscador Google como proveedor de contenidos como "de tratamiento de datos personales".

según el Tribunal Constitucional son "[…] los derechos del afectado a consentir sobre la recogida y uso de sus datos personales y a saber de los mismos. Y resultan indispensables para hacer efectivo ese contenido el reconocimiento del derecho a ser informado de quien posee sus datos personales y con qué fin, y el derecho a poder oponerse a esa posesión y uso requiriendo a quien corresponda que ponga fin a la posesión y empleo de los datos"[46]. Por lo tanto, el requisito indiscutible para todo tratamiento de datos personales será la exigencia del consentimiento. Este es el mecanismo que permite el control y disposición de nuestra propia información, algo que se denota esencial en el entorno virtual, donde los límites de espacio y tiempo desaparecen, ya que en internet siempre queda rastro de lo que hacemos, decimos, conocemos, etc., pudiendo ser esta información almacenada y utilizada sin ningún límite temporal, lo que dificultaría su control.

Desde el primer momento en el que pasamos por ejemplo a formar parte de una red social online, estamos suministrando información y datos personales, lo que en muchos casos nos podrá ayudar a desarrollarnos como personas libremente, pero que también supone un grave riesgo para nuestra vida privada, pudiendo afectar ya no sólo a nuestro derecho a la protección de datos personales sino también a otros muchos derechos.

Realmente si pensamos en el concepto de vida privada como tal, es algo totalmente opuesto a la finalidad de las redes sociales e Internet, ya que el requisito necesario de estas es compartir información con los demás usuarios de manera global. Por lo tanto, son sistemas abiertos, constituyéndose la misma con la información que cada usuario añade a su perfil, y esto sólo tiene cabida con su consentimiento[47]. Mayormente, el sujeto titular de los datos consiente voluntariamente el tratamiento de éstos y publica información personal suya, pero también se puede dar la situación, en la cual, este mismo usuario ofrezca información de terceros, sin que estos hayan podido prestar su consentimiento. Como afirma TRONCOSO, "la privacidad no trata sólo del respeto a nuestros datos personales, sino también del que debemos tener por la información relativa a los demás"[48]. Algo que no es compartido por el fundador de la red social "Facebook", MARK ZUCKERBERG, ya que según ARRINGTON, en una entrevista publicada en 2010, éste afirmaba que "la era de la privacidad había acabado"[49].

Dado que el consentimiento es la manifestación esencial del derecho fundamental a la protección de datos personales, debemos tener en cuenta que estamos hablando de la titularidad de un derecho fundamental. Al ser un derecho personalísimo, la única persona que puede prestar el consentimiento para que se traten estos datos es el propio titular de los mismos. Por lo tanto, la publicación en redes sociales e Internet de los datos personales, podría suponer una cesión

[46] STC (Pleno) de 30 de noviembre de 2000 (FJ 7º), (RTC 290, 2000).

[47] GARCÍA ESTÉVEZ, N: *Redes sociales en Internet. Implicaciones y consecuencias de las plataformas 2.0 en la sociedad*, Editorial Universitas, Madrid, 2012, pp. 41-42.

[48] TRONCOSO REIGADA, A: "Las redes sociales y la APDCM", en *Datos personales*, nº43, 2010, p.1.

[49] ARRINGTON, M: "Facebook's Zuckerberg Says The Age of Privacy is Over", en *Techcrunch,* 2010, pp.1-2.

de dichos datos, por lo que requerirá en consentimiento previo de los titulares, como determina al respecto el Memorándum de Montevideo, que recomienda a los servicios que proveen redes sociales: "no permitir la recopilación, tratamiento, difusión, publicación o transmisión a terceros de datos personales, sin el consentimiento explícito de la persona concernida. Se debe restringir el uso de la información recogida con cualquier otra finalidad diferente a la que motivó su tratamiento, y en especial a la creación de perfiles de comportamiento"[50].

Este requisito del consentimiento está regulado por la normativa Europea sobre el tratamiento de los datos personales y que tiene reflejo directo en nuestro ordenamiento jurídico, que es la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y en el Real Decreto 1720/2007[51], de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999. Por lo tanto, las redes sociales se encuentran sometidas a esta normativa de protección de datos, ya que el hecho de que el consentimiento se pase a prestar en otro medio diferente, como en este caso, no cambia la normativa aplicable, siempre que el objeto (datos personales) sea el mismo.

A las redes sociales les son de aplicación muchas de las previsiones nacionales y comunitarias sobre protección de datos personales, incluso si los proveedores de servicio están ubicados fuera de territorio nacional.

Como podemos observar, la normativa actual de datos personales se basa en la exigencia de consentimiento, pero esto ya no es suficiente, ya que son los destinatarios los que pierden el control de sus datos personales de forma voluntaria, y esto debido a que ese consentimiento no es tan libre ni tan consciente en la gran mayoría de ocasiones. Este cambio ya se está persiguiendo por Europa manteniendo que "conviene clarificar las condiciones del consentimiento del interesado, con el fin de garantizar que se conceda siempre con conocimiento de causa, y de garantizar que el interesado es plenamente consciente de que su autorización y respecto a que tratamiento"[52]. Por lo tanto, se hace necesaria una redefinición de consentimiento, adaptándolo a las nuevas realidades del cambio social y tecnológico del momento.

Como ya comentaba, conforme a la normativa Europea existente y a la española en vigor, el consentimiento es el requisito indispensable en relación con el tratamiento de datos personales, según expresa el art. 6 de la LOPD "El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, saldo que la ley disponga otra cosa". La LOPD además expresa las características que debe reunir dicho consentimiento, las cuales son: "toda manifestación de voluntad, libre, inequívoca, específica e informada", art. 3.h) LOPD y art. 5.1.d) RLOPD.

[50] Recomendación 25 del Memorándum de Montevideo el 3 de diciembre de 2009.

[51] BOE, núm. 17, de 19 de enero de 2008.

[52] Dictamen 15/2011, adoptado el 13 de julio, del G29, sobre *Definición del consentimiento* (011997/11/ES. WP 187).

Pero, algunas de estas características legalmente exigidas del consentimiento plantean problemas en el ámbito de las redes sociales e Internet. A continuación las analizaremos más detalladamente.

A) Libre

El consentimiento libre debe ser aquel que se otorga al margen de cualquier presión o coacción física o psíquica. Atendemos a la normativa civil al respecto establecida de los arts. 1262 a 1266 del CC, y más concretamente en su art. 1265 CC, que específica que "será nulo el consentimiento prestado por error, violencia, intimidación o dolo", y el art. 1266 CC, que existe error, cuando el mismo recae: "sobre la sustancia de la cosa que fuera objeto de contrato, o sobre aquellas condiciones de la misma que principalmente hubiesen dado motivo a celebrarlo".

El usuario en redes sociales normalmente publica todo tipo de información bajo la errónea creencia de que se encuentra en un entorno privado, es decir, entre amigos. La mayoría de estos servicios emplean conceptos como "amigos" ofreciendo así una falsa apariencia de privacidad en la que los usuarios confían y por lo tanto no temen en compartir todo tipo de información, por lo que el consentimiento se presta fruto de un error de partida[53].

Desde instancias europeas, se ha manifestado que: "el recurso al consentimiento debe limitarse a los casos en que el interesado tenga una auténtica libertad de elección y, por tanto, sea posteriormente capaz de retirar el consentimiento"[54].

Sería preciso por tanto, que los proveedores de redes sociales evitaran estas manifestaciones imprecisas sobre el entorno de las publicaciones de los datos personales, acompañándolo, por supuesto, de una correcta política de privacidad, la cual debería mostrar las consecuencias de no prestar el consentimiento al tratamiento de determinado tipo de información solicitada, y recordar a los usuarios la posibilidad de la revocación del mismo que inicialmente se prestó.

B) Informado

El usuario deberá ser informado previamente, para que pueda sopesar los riesgos y ventajas que le conlleva mostrar sus datos personales. Este requisito de información corresponde otorgarlo obligatoriamente al responsable del tratamiento de esos datos personales en el momento previo que se recogen los mismos (art. 5 LOPD). Por lo tanto, en el caso de las redes sociales, la obligación de informar corresponde a los proveedores de los servicios (suele

[53] FAERMAN, J: *Faceboom, el nuevo fenómeno de masas*, Alienta Editorial, Barcelona, 2010, pp. 33- 35.

[54] Dictamen 15/2011, de G29, pp. 14-17, que pone en duda que en el ámbito laboral o, con un ejemplo más concreto, en los escáneres de personas en los aeropuertos, las personas consientan libremente y no movidos para evitar posteriores sospechas o perjuicios.

ser a través de expresiones como "aviso legal" o "políticas de privacidad"). Respecto a esto, la AEPD pone de manifiesto que: "la manifestación de los requisitos legalmente exigidos al consentimiento del afectado se realizarán en la práctica a través de la información al afectado, en el momento de la recogida de sus datos de carácter personal, de los extremos esenciales relacionados con el tratamiento, recabando a tal efecto su consentimiento en relación con los aspectos especifica e inequívocamente hechos constar en la mencionada información"[55].

En relación con los buscadores de Internet, la LOPD añade que, " el tratamiento legítimo de los datos personales por los buscadores de Internet está sujeto a una condición previa tanto si se basan en la existencia de una relación jurídica, como si lo hacen en el consentimiento de quienes se registran voluntariamente para utilizar estos servicios: que las personas cuyos datos se tratan estén informadas de qué datos se van a utilizar, por quién, con qué finalidad y a quienes se pueden ceder sus datos"[56]. Por lo tanto, en este caso también es obligatorio una información previa. En estos casos una forma de obtener el consentimiento puede ser como un mero pronunciamiento donde el usuario participe activamente, de forma que a través de la web pueda manifestar su voluntad, pero según la AEPD: "para que la ausencia de manifestación de la voluntad del usuario pueda producir alguna consecuencia respecto del tratamiento de sus datos personales, deberá habérsele advertido expresamente de esta circunstancia, así como de los efectos del mismo"[57].

Pero, este tipo de mensajes debería de reunir características más sencillas, ya que no olvidemos que la mayoría de usuarios que contratan estos servicios, sobre todo las redes sociales, suelen ser en un alto porcentaje, adolescentes y menores de edad, y por lo tanto, su capacidad para creer que realmente están informados puede ser menor que la de un adulto. Por lo tanto, para poder considerar que se produce un consentimiento informado, los proveedores deberían de ofrecer una política de privacidad no demasiado extensa, fácilmente accesible, con un lenguaje sencillo y que fuera ineludible para continuar con el servicio.

C) Específico

Nuestros datos se tratan para una finalidad específica, es decir, para una actividad determinada, la cual el usuario consiente. En este sentido, la AEPD ha manifestado que "será nulo el consentimiento para la comunicación de los datos de carácter personal a un tercero cuando la información que se facilite al interesado no le permita conocer la finalidad a la que destinarán los datos

[55] Informe Jurídico 93/2008, de la AEPD, sobre Formas de obtener el consentimiento mediante web. Consentimientos tácitos.

[56] Declaración de la AEPD, sobre Buscadores de Internet, de 1 de diciembre de 2007.

[57] Informe Jurídico 0300/2009, de la AEPC; y Recomendación de la AEPD, sobre Comercio electrónico, de año 2000.

cuya comunicación se autoriza o el tipo de actividad de aquel a quien se pretenden comunicar"[58].

Normalmente los datos personales que el usuario publica suelen ir orientados a una finalidad concreta, como la relación con otros usuarios (amigos). Pero, el problema sucede porque, al ser información susceptible de ser compartida por estos usuarios (amigos), puede ser utilizada posteriormente para fines inespecíficos que no eran los iniciales y específicos del usuario supuesto contratador del servicio.[59]

Por lo tanto, sigo considerando la necesidad de constituir una adecuada política de privacidad. En este caso, y enlazándolo con el anterior requisito, el proveedor deberá de informar de forma más concreta el destino y destinatario final de la información suministrada.

D) Inequívoco

Este consentimiento debe de ser inequívoco, es decir, sin dejar lugar a duda o equivocación. Aunque esto sea así, el consentimiento tácito y presunto es admitido por la AEPD, ya que en la normativa existente en la materia no establece como obligatoria forma alguna de prestar consentimiento, rigiendo por lo tanto la libertad de forma. Por lo tanto puede prestarse de forma expresa (oral o escrito) o por actos reiterados del afectado que revelen que el mismo ha dado el consentimiento con dichos actos presuntos, o incluso por su silencio. Cosa que no sucede con los "datos sensibles"[60]. En este caso, no se considera que las imágenes en Internet sean datos sensibles, salvo si dichas imágenes se utilizan para revelar datos sensibles sobre las personas. Debemos ser cautos a la hora de utilizar este tipo de datos, ya que puede tener consecuencias no solo administrativas, si no también penales y/o civiles.

El problema que se da al admitir este consentimiento tácito, provoca que se puedan dar situaciones en las que, por ejemplo, parezca que un tercero ha dado su consentimiento por aparecer en una fotografía junto al usuario de la

[58] Recomendación de la AEPD sobre Comercio Electrónico del 2000.

[59] Como ha manifestado la AEPD en Buscadores de Internet, de 1 de diciembre de 2007: "Adicionalmente, en los casos en los que los usuarios de los servicios optan voluntariamente por registrarse como usuarios de servicios personalizados, la legitimación por el tratamiento de sus datos encontraría un fundamento específico basado en el consentimiento de los usuarios registrados. De lo expuesto debe concluirse que la legitimación para el tratamiento de datos de los usuarios afecta a las finalidades relacionadas directamente con el servicio de búsqueda, como son la prestación y mejora del mismo, la seguridad, la detección de fraudes y la facturación. Si bien, la utilización de los datos personales que se lleva a cabo debe ser proporcionada, en cada caso, a la finalidad que la justifique". Si se modifica la finalidad para la que se han recogido nuestros datos y no se nos informa, nuestro consentimiento deja de ser específico, cayendo además, más que probablemente, en la prohibición de utilizar los datos para finalidades incompatibles, tal y como señalo la SAN (Pleno) de 27 de abril de 2006 (STC 132, 2006).

[60] Pero hay determinados datos personales que requieren un consentimiento expreso, incluso en escrito en algún supuestos, como son los denominados "datos sensibles" establecidos en el art. 7 de la LOPD.

red social, y sin embargo, este sujeto no sea consciente del tratamiento que el citado usuario está realizando con su imagen.

Por lo tanto, y según afirman ARTEMI RALLO y RICARD MARTÍNEZ, lo aconsejable en los servicios de redes sociales e Internet, sería no admitir un consentimiento tácito, debiendo exigir los responsables del tratamiento de datos un consentimiento expreso. Pero como actualmente no es así, solo queda exigir a los responsables del tratamiento que tomen todas las cautelas posibles, analizando los casos para entender que se ha producido y si realmente se ha otorgado el consentimiento[61].

E) Previo

A pesar de que este requisito no aparece expresamente en la definición del consentimiento que establece la LOPD, con ella se hace referencia al momento en el cual el consentimiento tiene que darse. Es lógico, que el consentimiento debe de prestarse antes de que se produzca el tratamiento de datos personales, justo en el momento en el que se procede a la recogida de dichos datos, previamente y según lo establecido en la normativa (art. 5.1 y 5.4 LOPD).

Como regla general, en los servicios de redes sociales e Internet, la recogida de datos se origina en el momento en que el interesado se da de alta vía web. Es el responsable, salvo excepción, el que deberá solicitar el consentimiento del usuario de los datos para su tratamiento.

El problema se origina cuando este tratamiento de los datos se realiza, no por el proveedor del servicio red, si no por los usuarios del mismo, cuando publican datos de terceros. En este tipo de casos, el consentimiento de los terceros también tendría que ser previo. Pero, diversos autores, como HOLAND, y SALVADOR CODERCH, consideran que debido a la dificultad de estos casos, para no obstaculizar el funcionamiento de las redes, este requisito legal debe interpretarse de una forma más flexible[62].

Aunque en mi opinión, considero que cualquier tratamiento de datos que se realice en este ámbito debería ser previamente consentido, y si no, no deberían de tratarse dichos datos.

F) Revocable

Este requisito tampoco aparece expresamente en la definición de consentimiento de la LOPD, pero si implícitamente, ya que ésta lo determina como una facultad que posee el usuario de los datos (art. 6.3 LOPD). El

[61] RALLO, A; MARTÍNEZ, R: *Derecho y redes sociales 2ª Edición,* ed: Thomson Reuters, Navarra, 2013, p. 176.

[62] HOLAND, B: "Privacy Paradox 2.0", en *Widener Law Journal*, Vol. 19, nº3, 2010, p. 38. SALVADOR CODERCH, P: "Imágenes veladas. Libertad de información, derecho a la propia imagen y autocensura de los medios", en *InDret*, nº 1, 2011, p.3.

usuario de los datos tratados a través de su consentimiento, puede en cualquier momento revocar el mismo[63].

Aquí encontramos el problema de que, los datos personales ya se han visto "colgados" o publicados en una red, y hemos de saber, que en el momento en el que se publican datos puede perderse el control de los mismos, ya que es imposible saber y controlar el número de personas que han accedido a ellos y, a su vez, cuantos la han comunicado a otros terceros, y estos a su vez a otros, y así sucesivamente. Lo que provoca que no sea muy efectiva la eliminación de los datos personales del usuario una vez que revoque el consentimiento.

Por lo tanto, sería recomendable que las políticas de privacidad fueran accesibles a los usuarios pudiendo así eliminar sus datos de los servidores cuando desactivaran su perfil, y además que los proveedores comunicaran a sus usuarios que si un tercero les solicita suprimir la información de su persona, estos deberían proceder a su borrado.

5.1 Menores e incapacitados

Este tema estaba regulado por el Código Civil en su art.315, el cual marca como 18 años la mayoría de edad, recogiéndose en los arts. 162,163 y 222 la representación legal para el caso de menores e incapacitados. En principio, y como afirma el art. 1263 del CC en virtud de la modificación establecida por la Ley 26/2015, de 28 de julio, de modificación del sistema de protección a la infancia y a la adolescencia[64], "no pueden prestar consentimiento: 1º los menores no emancipados, salvo en aquellos contratos que las leyes les permitan realizar por sí mismos o con asistencia de sus representantes, y los relativos a los bienes y servicios de la vida corriente propios de su edad de conformidad con los usos sociales. 2º los que tienen su capacidad modificada judicialmente, en los términos señalados por la resolución judicial". Pero, como establece en la actualidad el art. 162 CC y conforme el apartado 12 del artículo 2º de la Ley 26/2015, la cual modificó dicho artículo, "Los padres que ostenten la patria potestad tienen la representación legal de sus hijos menores no emancipados. Se exceptúan: 1º Los actos relativos a los derechos de la personalidad que el hijo, de acuerdo a su madurez, pueda ejercitar por sí mismo. No obstante, los responsables parentales intervendrán en estos casos en virtud de sus deberes de ciudadano y asistencia". Por lo tanto, no tendrán representación legal de los hijos no emancipados en aquellos actos que se refieran a los derechos de la personalidad del hijo. Con la entrada en vigor del RLOPD se desarrolla y completa la materia y se considera que los mayores de 14 años podrán prestar el consentimiento al tratamiento de sus datos personales, sin que sea necesario el consentimiento de sus padres o tutores legales (art. 13 RLOPD). Pero la AEPD ha mantenido que: "es necesario recabar el consentimiento de los menores para la recogida de sus datos […]

[63] La revocación no debe de confundirse con la solicitud de cancelación de los datos porque éstos no cumplan con los requisitos de actualización, exactitud y conservación.

[64] BOE, núm. 180, de 29 de julio de 2015.

recabándose en caso de mayores de catorce años cuya madurez no garantice la plena comprensión por los mismos del consentimiento prestado, el consentimiento de sus representantes legales"[65].

El problema es que una gran cantidad de usuarios de las redes sociales e Internet son menores de edad, convirtiéndose cada vez más en una actividad habitual para su desarrollo social. Por lo que cada vez son más jóvenes los que se enfrentan a innumerables peligros, lo cual supera con creces a las ventajas que las redes sociales e Internet pueda ofrecerles. Aunque como garantías jurídicas tengamos las Leyes Orgánicas 1/1982, de Protección de Honor, Intimidad y Propia Imagen, así como la 1/1996, de Protección Jurídica del Menor, junto a otras comunitarias e internacionales, el fenómeno de las redes sociales está desbordando el paraguas de protección que a estos usuarios se les ofrece.

Las únicas garantías que ofrece la normativa a estos usuarios es, por un lado que el lenguaje empleado sea más sencillo y comprensible para aquellos, y por otro, que el responsable del fichero garantice que ha comprobado la edad del menor y la autenticidad del consentimiento (art. 13.3 y 4 RLOPD). En la actualidad este último aspecto es muy difícil controlarlo, a pesar de ello, se están implantando nuevos sistemas de reconocimiento de DNI electrónico y además, un papel muy importante lo juegan los padres o tutores, los que establecerán controles y filtros para el acceso a diversas redes e Internet en los dispositivos electrónicos de los menores.

Respecto a los incapaces, se incluirían en el mismo grupo de los menores, ya que las reglas relativas a tutela, curatela y guarda prevista en el CC, rige igualmente para los incapaces. Por lo tanto, si no son capaces de prestar ellos mismos su consentimiento, deberán ser sus representantes legales los que lo presten por ellos, por lo que para estos casos no existe límite de edad, sino únicamente el fijado por sentencia judicial firme[66].

5.2 Fallecidos

Respecto a las personas fallecidas, atendemos a la normativa civil y al hecho de que el derecho a la protección de datos se constituye como un derecho personalísimo, por lo que se considera que no pueden ser titulares de estos derechos las personas fallecidas, es decir, no se le puede otorgar un derecho de protección de datos personales a una persona que esta fallecida.

A pesar de esto, la AEPD afirma que aunque el derecho a la protección de datos es personalísimo y el cual la persona fallecida pierde, los familiares de esa persona si podrán ejercer un derecho de acceso o cancelación,

[65] Informe Jurídico de la AEPD 2000/0000, sobre El consentimiento otorgado por los menores de edad.

[66] Arts. 199-214 CC. Según el citado Código: "son causas de incapacitación las enfermedades o deficiencias persistentes de carácter físico o psíquico que impidan a la persona gobernarse por sí misma" (art. 200).

convirtiéndose esto en la vía alternativa que tendrían las terceras personas distintas al usuario para garantizar los derechos del familiar fallecido.

En la actualidad, las redes sociales más populares, como por ejemplo Twitter, cuentan con protocolos de eliminación de perfiles de fallecidos, dando incluso la posibilidad de crear un perfil conmemorativo. Para que esto se pueda llevar a cabo, los responsables de las redes sociales exigen una prueba documental con el fin de verificar que el solicitante es un familiar del causante (certificado de defunción).

El protocolo de eliminación de perfiles de fallecidos en las redes sociales como es Twitter está disponible en el siguiente enlace:

http://support.twitter.com/articles/20169203-como-comunicarse-con-twitter-para-informar-sobre-un-usuario-fallecido[67].

5.3 Excepciones al consentimiento y su repercusión en el uso de las redes sociales e internet

A pesar de que, como ya comentaba anteriormente, el consentimiento es un requisito esencial para el tratamiento de datos personales, existen algunas excepciones sobre el mismo, establecidas en el art. 6.2 de la LOPD.

La primera excepción a la regla general es en el supuesto de que la Ley disponga otra cosa, lo que significa que al entrar en conflicto de intereses jurídicamente protegidos deberá realizarse una ponderación entre ellos. Junto a esta excepción la LOPD recoge un conjunto de supuestos en los que no es necesario el consentimiento del usuario. Estos son los siguientes:

A) Funciones propias de las Administraciones Públicas

En este caso no es necesario el consentimiento para el ejercicio de funciones que realice la Administración pública en el ámbito de sus competencias, pero para ello hay que estar a lo dispuesto en la normativa sobre competencia y atribución de funciones. El Estado es el que determina si el responsable del tratamiento de los datos que tiene conferida la misión de interés público, debe ser la Administración pública u otra persona de derecho público o privado como, por ejemplo, una asociación profesional[68].

B) Partes de un contrato

Se refiere a las partes de un contrato o precontrato de una relación ya sea, negocial, laboral o administrativa, ya que se entiende que existe un consentimiento previo o que se otorgó en el momento de la formalización del contrato o de la relación negocial, laboral o administrativa, siendo

[67] ÁLVAREZ, J: "Internet, redes sociales y protección de datos", *Aranzadi, SA*, 2014, p. 1.

[68] Directiva 95/46/CE, art. 7.e). (DOUE L281 de 23 de noviembre de 1995).

lógico que no se exija consentimiento cuando se quiera solamente el mantenimiento o cumplimiento de la misma.

Por lo tanto, si un titular se adhiere a una red social y acepta voluntariamente sus condiciones de uso, esa aceptación se entiende como un consentimiento tácito. Entre el usuario y el proveedor de la red social se establece una relación jurídica en la que el proveedor tratará sus datos sin necesidad de consentimiento (siempre que sea para su mantenimiento o cumplimiento de la relación y no para otra finalidad).

C) Interés vital

Tampoco se necesitará en consentimiento cuando se pretenda con el tratamiento de datos personales proteger un interés vital del interesado (art. 6.2 LOPD).

D) Fuentes accesibles al público y satisfacción del interés legítimo del responsable

No será necesario el consentimiento cuando los datos figuren en fuentes accesibles al público (censo promocional, boletines oficiales, repertorios telefónicos, etc) y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero, siempre que no vulneren los derechos y libertades fundamentales.

Internet no es una fuente de acceso público y los servicios que se prestan a través de la misma tampoco tienen dicha consideración[69], como es el caso de las redes sociales, estas no están amparadas por la excepción y requerirá por lo tanto previo consentimiento[70].

E) Cesión de datos conforme a circunstancias legales y reglamentarias

El art. 11.2 de la LOPD y el art. 10.4 RLOPD determinan que no será necesario el consentimiento cuando se produzca una cesión de datos personales en las circunstancias legales y reglamentarias determinadas, como por ejemplo, en la cesión de datos entre Administraciones Públicas, o cuando el destinatario sea el Defensor del Pueblo, el Ministerio Fiscal, el Tribunal de Cuentas o Jueces y Tribunales.

F) Exención doméstica.

Se entiende por finalidad doméstica según la RLOPD y los Informes de la AEPD, que recogen la jurisprudencia de la Audiencia Nacional que: "el

[69] LESMES SERRANO, C*: La Ley de Protección de Datos. Análisis y comentario de su jurisprudencia,* Lex Nova, Valladolid, 2008, p. 12.

[70] Así se pronunció SAN de 18 de mayo de 2006 (SAN (Sala 1º), de 18 de mayo de 2006 (530,2004)) al considerar que el hecho de que el nombre y dirección de una persona, a la que se le envió publicidad promocional, apareciera en el buzón de cada domicilio y fuera expuesta al público, no puede confundiré con que dichos datos sean una fuente de acceso público.

tratamiento realizado por una persona física en el marco de una actividad exclusivamente privada de imágenes de terceros a través de Internet en abierto. Por lo que para la captación de imágenes de acuerdo con lo previsto en la LOPD será de aplicación los principios de legitimación o consentimiento, de información, de seguridad y el deber de secreto"[71].

Por lo que es el caso en el que se estén realizando actividades exclusivamente personales o domésticas. Así, si un sujeto trata datos de terceros con una finalidad doméstica, no tendría que exigirles su consentimiento, pero, en el caso de que en Internet o en las redes sociales se lleve a cabo su publicación, estaría extralimitando esa actividad exclusivamente doméstica.

Por lo tanto, para que nos encontremos ante una exclusión normativa, es necesario que nos estemos refiriendo a actividades exclusivamente profesionales o familiares, equiparables a las que podrían llevarse a cabo si no hiciéramos uso de Internet. De este modo, se afirma que la publicación por ejemplo de fotografías en páginas web, a las que tiene acceso cualquier sujeto, va más allá del ámbito meramente familiar o personal, por lo que no se encontraría dentro de las excepciones legalmente previstas.

5.4 El consentimiento y las políticas de privacidad

Todas las redes sociales y las plataformas virtuales son conscientes de los peligros que puede ocasionar el uso de sus plataformas, por lo que advierten de ello en sus páginas y recomiendan un uso responsable de las mismas estableciendo la posibilidad de elegir entre diferentes niveles de privacidad, limitando por lo tanto, a los usuarios el acceso de sus datos o información. Pero, existen algunos datos (generalmente los del perfil del usuario) que serán públicos para todo el mundo, sin que exista posibilidad de establecer esa privacidad. Esto sería por ejemplo aquellas fotografías que se publican en el perfil, que forman parte de lo que las redes sociales, y como Facebook denomina: "información que está disponible siempre públicamente"[72], pudiendo acceder a ellas todo el mundo, hasta que el usuario las elimine del perfil[73].

---

[71] Art. 4.a) RLOPD; e Informe de la AEPD, al hilo de la Inspección Sectorial de Oficial de Videocámaras en Internet, de 2009.

[72] CORREDOIRA, L; COTINO, L: *Libertad de expresión e información en Internet: amenazas y protección de los derechos personales*, ed: Centro de Estudios Políticos y Constitucionales, Madrid, 2013, p.444.

[73] Según afirma Facebook en su plataforma: "Fotos de perfil y fotos de portada: Ayudan a tus amigos y familiares a reconocerte. Si no te gusta publicar ninguna de esas fotos, siempre puedes borrarlas. A menos que las elimines, cuando añadas una nueva foto del perfil o foto de portada, la foto anterior continuará siendo pública y permanecerá en el álbum de fotos del perfil o de fotos de portada", lo que significa que: "- que puede asociarse contigo (es decir, tu nombre, fotos del perfil, fotos de portada, biografía, identificador de usuario, nombre de usuario, etc), incluso fuera de Facebook; - que puede mostrarse cuando alguien hace una búsqueda en Facebook o en un motor de búsqueda público;- que estará accesible

Además indican que la información y/o imágenes que los usuarios cuelgan en la red, no son controlables, aunque se haya establecido por el mismo usuario un nivel muy alto de privacidad, pues ese nivel sólo se refiere a su perfil, pero no al de aquellos que tienen acceso a su información y pueden descargarla. Según ROMERO: "robar una foto en Facebook es muy fácil: lo único que hay que haces es arrastrar la imagen con el puntero a la barra de navegación y así se puede obtener la dirección de la misma. Cualquiera, tenga o no cuenta en la red social, puede verla"[74]. Esto no se trata de un agujero en la seguridad, sino un problema de privacidad que sucede porque la compañía deposita imágenes en servidores públicos de fotos contratados para ello. La configuración de privacidad de los usuarios, por ejemplo en Facebook, no se aplica a los servidores que depositan la foto, sino que sólo sirven para limitar quién puede ver el enlace a la foto en el servidor de fotos, por lo tanto, todas las fotos están a disposición del público sin tener en cuenta la configuración de la privacidad individual que el usuario selecciona.

Es cierto, que el que "tus amigos" tengan acceso a tus imágenes es peligroso, pero más peligroso aún es que las propias redes sociales se apropien del derecho a usarlas y ceder su uso a terceros, como manifiestan estos servidores en el apartado dedicado a la política de uso de datos (condiciones que debes aceptar para poder registrarte), donde se explica a los usuarios que al publicar sus fotos están cediendo sus derechos de autor a la plataforma virtual (aunque no de forma exclusiva)[75]. La información y los datos que se filtran en Internet tienen un gran valor económico para las empresas, de hecho, la empresa Facebook disfruta de una posición privilegiada en el mercado, ya que éste usa nuestros datos personales para crear un perfil de usuario al que las empresas de publicidad puedan dirigir sus campañas, pero con la futura entrada del Reglamento general de protección de datos, el usuario podrá oponerse lo que podría afectar notablemente al negocio publicitario que Facebook tiene montado con la creación de perfiles de sus usuarios con fines comerciales[76].

---

para los sitios web, aplicaciones y juegos integrados en Facebook que utilizáis tú y tus amigos;- que será accesible para cualquiera que utilice nuestras API de la gráfica social".

[74] ROMERO, P: "La engañosa privacidad de las fotos de Facebook", en *El Mundo*, 2011, p.1.

[75] Según afirma Facebook: "Eres el propietario de todo el contenido y la información que publicas en Facebook, y puedes controlar cómo se comparte a través de la configuración de la privacidad y de las aplicaciones. Además:- para el contenido protegido por los derechos de propiedad intelectual, como fotografías y vídeos, nos concedes específicamente el siguiente permiso, de acuerdo con la configuración de la privacidad y las aplicaciones: nos concedes una licencia no exclusiva, transferible, con derechos de subsidencia, libre de derechos de autor, aplicable globalmente, para utilizar cualquier contenido de PI que publiques en Facebook o en conexión con Facebook (licencia IP). Esta licencia de PI finaliza cuando eliminas tu contenido de PI o tu cuenta, salvo si el contenido se ha compartido por terceros y estos no lo han eliminado;- cuando eliminas contenido de PI, este se borra de forma similar a cuando vacías la papelera de reciclaje de tu equipo. No obstante, entiendes que es posible que el contenido eliminado permanezca en copias de seguridad durante un plazo de tiempo razonable (si bien no estará disponible para terceros".

[76] GARCÍA, L: "¿Utiliza Facebook nuestros datos personales?", en *Centro de Estudios de Consumo*, 2016, pp. 6-7.

Pero los derechos de propiedad intelectual no son sinónimo de derecho a la propia imagen, así, aunque se consideren cedidos aquellos, el consentimiento sobre el uso de nuestra imagen es revocable en cualquier momento, y además, si se trata de imágenes de menores y su uso le perjudique, podrá intervenir incluso el Ministerio Fiscal. Sería recomendable, desde mi punto de vista, que estas plataformas recabaran el consentimiento del menor o de la persona responsable del mismo cada vez que la imagen se usara para un fin diferente, puesto que de la misma manera que el consentimiento dado para ser fotografiado no es equiparable al dado para que la imagen sea difundida, tampoco debería presumirse validez a un consentimiento dado para aparecer en el perfil de una plataforma que para aparecer en circunstancias diferentes. Por lo tanto, el hecho de subir una fotografía de una persona en el perfil de una red social, no puede deducirse un consentimiento válido para difundirla en lugares y para fines diferentes, ya que cada uno de estos actos necesitaría, a mi parecer, un consentimiento específico.

5.5 El consentimiento informado del usuario para la instalación de cookies

Normalmente el usuario, a pesar de los anuncios referentes a las cookies, sigue navegando y utilizando la red aunque no entienda con precisión lo que significan. En España, en la encuesta realizada por la Asociación para la investigación de medios de comunicación, "Navegantes en la red", sobre las cookies a 33.254 encuestados, a la pregunta sobre como tienen configurado su navegador en relación con las cookies, es decir, si las acepta o rechaza, sólo el 7.5% afirmó que las rechazaba o bloqueaba, un 16% no sabía de qué se trataba y el resto las admitía aunque no supiera de que se trataba. Además un 49.2% sostenía la necesidad de solicitar el consentimiento previo antes de que sean instaladas en el equipo[77].

El término cookies según el vocablo inglés se traduce por "galletas", pero también se denomina como "chivatos". Las cookies son "pequeños archivos que algunos sitios web guardan en tu ordenador […]. La cookie es un texto alfanumérico que se descarga en el equipo terminal del destinatario de la prestación de un servicio de la sociedad dela información cuya función es almacenar datos en el mismo que pueden ser recuperados por el prestador del servicio cuando el destinatario vuelve a solicitar la información, esto es, vuelva a conectar con el sitio web o con otro que forma parte de la misma red"[78], por lo tanto, su función consiste en almacenar información sobre el usuario en su terminal, es decir, si el usuario tiene una cookie de un sitio web al que va muy a menudo, la cookie recuerda cosas que harán tu próxima visita a esta página web mucho más fácil. Estas pueden ser temporales, denominadas como "cookies de sesión"[79] o permanentes, denominadas como

[77] ASOCIACIÓN PARA LA INVESTIGACIÓN DE MEDIOS DE COMUNICACIÓN: "*Navegantes en la red",* 2013. p.1.

[78] NAVAS, S: *La personalidad virtual del usuario de internet: Tratamiento de la información personal recogida mediante cookies y tecnología análoga*, ed: Tirant lo Blanch, Madrid, 2014, pp. 27-28.

[79] Permite recoger y almacenar datos en el equipo mientras el usuario accede a un sitio web.

"cookies persistentes". En estas últimas, la entidad titular de la cookie puede acceder a ellas durante un periodo de tiempo que esta misma defina, pudiendo variar en días, meses o años[80].

Las primeras cookies eran de carácter meramente técnico con la finalidad de facilitar el servicio, como por ejemplo, recordar su contraseña, no obstante, en la actualidad la información suministrada por ellas podría servir para otras finalidades, tales como la de elaborar un perfil del usuario y enviarle publicidad de acuerdo con el mismo.

Respecto a la obligación de informar, viene reflejada en el art. 22.2 LSSICE que establece el deber que tienen los prestadores de servicios de la sociedad de información de facilitar a los usuarios la información de forma clara y completa sobre la utilización de archivos de recogida, almacenamiento y recuperación de los datos, y sobre todo de las finalidades perseguidas con tales tratamientos de acuerdo con lo establecido por la LOPDCP. Se trata pues de una obligación legal de hacer, por lo que el titular del derecho a exigir la información (usuario) puede exigir judicialmente su cumplimiento, según el art. 1098 CC, y si no lo hiciera, podrá ejecutar a su costa, conforme al art. 706 LEC. Además, aquel usuario afectado por la falta de información tendría la opción de presentar una reclamación ante la AEPD (art. 117 RDCP) o incluso exigir la indemnización de los daños, generalmente morales, ocasionados por la instalación del dispositivo sin información previa (art. 1902 CC, art. 9 LOHIPFPI, art. 19 LOPDCP). Es una obligación unilateral (una obligación de aquel que desea instalar la cookie) y tiene carácter previo a la prestación del consentimiento. Por lo tanto, esta obligación de informar incluye el deber de proporcionar toda aquella información que imponga el principio general de buena fe y que evite el dolo (art. 7.1 CC). Además, es una obligación cuyo cumplimiento es de tracto sucesivo, por lo que la información debe estar siempre disponible para el usuario, informándosele de los cambios o actualizaciones.

Como ya comentábamos, el art. 22.2 LSSICE, establece la necesidad de que medie el consentimiento del usuario del servicio para proceder a la instalación de cookies, debiendo ser previo. Sin embargo, este precepto exceptúa de la necesidad de ese consentimiento a determinado tipo de cookies, como son aquellas de índole técnica, estableciéndolo así: "lo anterior no impedirá el posible almacenamiento o acceso de índole técnica al solo fin de efectuar la transmisión de una comunicación por una red de comunicaciones electrónicas o, en la medida que resulte estrictamente necesario, para la prestación de un servicio de la sociedad dela información expresamente solicitado por el destinatario". A pesar de esto, la norma no establece la no necesidad de informar al destinatario del servicio, sino tan sólo que no se requiere que

[80]La aplicación "LinkedIn" por ejemplo, usa estos dos tipos de cookies. Una cookie permanente se almacena cuando inicias sesión en tu cuenta. La próxima vez que visites el sitio web de LinkedIn utilizando el mismo aparato, la cookie permanente nos permitirá reconocerte como usuario, por lo que no necesitarás iniciar la sesión para utilizar sus servicios. En cambio, la cookie de sesión se utiliza para identificar una visita particular al sitio web de LinkedIn, caducando cuando cierras tu navegador (http://www.linkedin.com/legal/cookie-policy?trk=hb_ft_cookie).

preste su consentimiento. No obstante, la Directiva 2009/136/CE en su número 66, parece extender la exención del consentimiento a la obligación de informar. Por lo tanto, existen cookies que quedan exceptuadas de la necesidad de proporcionar información y de exigir consentimiento del usuario, y otras que no lo están.

El consentimiento del usuario del servicio web debe configurarse jurídicamente como se configura el consentimiento del afectado por el tratamiento de datos personales. Este consentimiento no se puede calificar como contractual, ya que no nace ninguna relación jurídica (no han celebrado ningún contrato), si no que se hace en el sentido de "asentimiento". El asentimiento del usuario se configura como una declaración de voluntad unilateral y recepticia cuya finalidad es legitimar la actuación del titular de la cookie que se introduce en la esfera privada de aquel y la de dar eficacia jurídica a la declaración de voluntad unilateral. Este sentido de "consentimiento" es el mismo que debe atribuirse al consentimiento informado en caso de tratamiento de datos personales, por lo que tampoco nade una relación jurídica entre las partes[81]. Sin esta autorización, el (servidor) no podría ejercitarlo y si lo hiciera estaría cometiendo una intromisión ilegítima que daría lugar a la indemnización oportuna.

6. El derecho al olvido en internet

El nacimiento de las Redes ha afectado de forma directa al Derecho, dando pie al nacimiento de nuevas especialidades del mismo como el Derecho de las TIC (nuevas tecnologías de la información y comunicación) o el Derecho digital. Asimismo la Administración de Justicia se está digitalizando, admitiendo nuevos medios probatorios en los juicios por la llamada prueba electrónica[82]. Pero, a pesar de que esta disciplina ha ido incorporando cambios a la vez que se producía el fortalecimiento de Internet, siempre ha ido por detrás de los avances tecnológicos. Como mencionada LAWRENCE LESSIG en su conferencia On the future of IP Law, primero aparece la tecnología y luego es el Derecho el que intenta adaptarse a ella[83]. De hecho, es en el campo de los derechos fundamentales relativos al derecho a la intimidad y protección de datos personales, donde se plantean unos importantes retos respecto a una normativa eficaz, ya que nos encontramos un marco regulador adecuado y armonizado.

En España, este problema apareció como consecuencia de las quejas que emitían los ciudadanos dirigidas a AEPD, que pretendían que los motores de búsqueda, como por ejemplo Google[84], dejaran de indexar informaciones que contenían datos

[81] APARICIO, J: *Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal*, 3ª Edición, ed. Aranzadi-Thomson Reuters, 2009, pp. 20 y ss.

[82] ÁLVAREZ CARO, M: *Derecho al olvido en Internet: El nuevo paradigma de la privacidad en la era digital,* ed: Reus S.A, Madrid, 2015, p. 17.

[83] LAWRENCE, L: *Digital Law World Congress: On the future of IP Law*, Barcelona, 2012, p.1.

[84] Google es una compañía estadounidense la cual ofrece este servicio como motor de búsqueda a través de la red. El 87% afectan al motor de búsqueda de Google, según la Memoria de la AEPD correspondiente al año 2009.

personales, es decir, que dejaran de realizar un tratamiento de datos personales de diversos usuarios ya que afectaba a sus intereses legítimos (intimidad personal y familiar, honor y dignidad entre otros).

Podríamos plantearnos las siguientes preguntas ¿los usuarios deben resignarse a soportar que sus datos personales permanezcan *sine die* en Internet al alcance de cualquiera en un buscador? ¿Cuánto tiempo debe soportarse este acceso universal a los datos personales? Este, es uno de los grandes retos de este siglo, lo que ha provocado la aparición del denominado Derecho al Olvido.

El Derecho al Olvido es aquel derecho que tienen las personas frente a los motores de búsqueda para que eliminen los datos personales de los mismos cuando esa información ya esté obsoleta, no sea adecuada, o es irrelevante para el interés público.

Está claro que Internet no falla en su memoria frente a la memoria humana, por eso en enero de 2012, la Comisión Europea aprobó una propuesta de Reglamento para la protección de datos en el que contempla el Derecho al Olvido digital, concretamente en su art.17, el cual establece:

> "1. El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos personales cuando concurra alguna de las circunstancias siguientes: a) los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo; b) el interesado retire el consentimiento en que se basa el tratamiento de conformidad con el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), y este no se base en otro fundamento jurídico; c) el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 1, y no prevalezcan otros motivos legítimos para el tratamiento, o el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 2; d) los datos personales hayan sido tratados ilícitamente; e) los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento; f) los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información mencionados en el artículo 8, apartado 1.
>
> 2. Cuando haya hecho públicos los datos personales y esté obligado, en virtud de lo dispuesto en el apartado 1, a suprimir dichos datos, el responsable del tratamiento, teniendo en cuenta la tecnología disponible y el coste de su aplicación, adoptará medidas razonables, incluidas medidas técnicas, con miras a informar a los responsables que estén tratando los datos personales de la solicitud del interesado de supresión de cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos.
>
> 3. Los apartados 1 y 2 no se aplicarán cuando el tratamiento sea necesario: a) para ejercer el derecho a la libertad de expresión e información; b) para el cumplimiento de una obligación legal que requiera el tratamiento de datos impuesta por el Derecho de la Unión o de los Estados miembros que se aplique

> al responsable del tratamiento, o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable; c) por razones de interés público en el ámbito de la salud pública de conformidad con el artículo 9, apartado 2, letras h) e i), y apartado 3; d) con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, en la medida en que el derecho indicado en el apartado 1 pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento, o e) para la formulación, el ejercicio o la defensa de reclamaciones."

Es a partir de este Reglamento general cuando se configura por primera vez el Derecho al Olvido como un derecho autónomo a los denominados "Derechos ARCO" (Acceso, Rectificación, Cancelación y Oposición). Su objeto proviene del contenido del derecho de cancelación, según se aplicaba en la Directiva europea de privacidad y de las normas nacionales[85].

Como podemos observar, las grandes ventajas de las tecnologías de la información, producen también grandes inconvenientes, como es el hecho de almacenar millones de datos de forma indefinida en una plataforma, como los grandes motores de Internet los cuales con frecuencia emiten informaciones que debían haber sido borradas por no ajustarse con datos reales o actualizados. Pero reclamar este derecho a una empresa por ejemplo como es Google, es muy complejo. Hasta ahora, reclamaciones que han sido planteadas en Francia o Italia han sido derivadas a los tribunales de Estados Unidos (California), donde Google tiene su sede. Esta empresa ha alegado que, al estar ubicado allí, está sometido a la jurisdicción norteamericana en materia de protección de datos, pero la Audiencia Nacional, así como la Agencia Española de Protección de Datos, afirman que la tutela de derechos fundamentales no puede depender del lugar que el gestor del buscador haya elegido para ubicarse[86].

No fue hasta el año 2014 por la STJUE de 13 de mayo de este mismo año, (Asunto C-131/12) cuando el Tribunal de Justicia de la Unión Europea falló en este sentido y constituyó el derecho a requerir la retirada de dicha información de la red. Esta sentencia, la cual originó el Derecho al Olvido, determinaba que "si bien el tratamiento de datos personales que se llevaba a cabo por la entidad estadounidense como sociedad matriz (Google Inc.), la filial española Google Spain resultaba responsable por el tratamiento de los datos personales en cuanto realiza esta actividad en el marco de las actividades de la sociedad matriz, lo que quiere decir que no se precisa que el tratamiento de datos personales sea

[85] Directiva 95/46/CE, de 24 de octubre de 1995, relativa a la protección de las personas físicas a lo que respecta al tratamiento de datos personales y la libre circulación de estos datos (DOCE L281 de 23 de noviembre de 1995), derogada actualmente por el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 (DOUE de 4 de mayo de 2016).

[86] REGLERO, F; BUSTO, M: *Tratado de Responsabilidad Civil*, Tomo II, 5ª edición, ed: Thomson Reuters Aranzadi, Navarra, 2014, pp.1417-1418.

efectuado por el propio establecimiento, sino que es suficiente que se realicen por una filial en el marco de sus actividades"[87].

Pero la Sentencia (Sala 3ª) del TS, de 14 de marzo de 2016 introduce una novedad jurisprudencial en relación a este derecho. La Sala de lo Contencioso del TS entiende que la filial española de Google no debe ser responsable del tratamiento de datos personales ya que afirma que es responsable Google Inc. (estadounidense), como sujeto que determina los fines y los medios del tratamiento de los datos personales, declarando que la promoción de productos o servicios publicitarios en beneficio del responsable realizada por Google Spain, es una actividad ajena a la determinación de los fines y medios del tratamiento, como afirma RALUCA" la responsabilidad de quien realiza la gestión del motor de búsqueda no puede ser trasladada a quien realiza actividades que tengan que ver con el soporte económico del motor de búsqueda, ya que no participa de una forma concreta en una actividad directamente vinculada a la indexación o almacenamiento de información o datos"[88]. Además descarta la unidad de negocio respecto a ambas sociedades, como argumento justificativo de su corresponsabilidad.

Pero la Sala de lo Civil del Tribunal Supremo, en la STS (Sala 1ª) de 5 de abril de 2016 (RJ 2016,1006) afirma lo contrario, considerando a Google Spain responsable por vulnerar su derecho a la protección de datos personales por no retirar de su buscador la información relativa a un indulto concedido en 1999. La sentencia desestima la alegación de Google Spain de "considerar a la sociedad matriz Google Inc. única responsable del tratamiento de los datos y argumenta que esa solución supondría en la práctica un serio obstáculo para la efectividad de los derechos fundamentales en cuanto el afectado debería litigar contra la sociedad matriz estadounidense lo que supondría la dilación del procedimiento y unos gastos elevados". Aun así, la Sala de lo Civil, ha tenido en cuenta las recientes sentencias de la Sala de lo Contencioso-Administrativo del mismo Tribunal, que estimaron la falta de legitimación alegada por la empresa española, concluye que no tienen efecto prejudicial sobre el recurso que resuelve la Sala de lo Civil por la existencia de diferentes criterios rectores en la jurisdicciones civil y contencioso administrativo y por la diversidad de las normativas que se aplican por unas y otras.

A pesar de esto, y a pesar de que Google, trabaja incesantemente en las peticiones que le llegan, no siempre actúa como establecen las normativas al respecto, de hecho, la Comisión Nacional de Informática y Libertades de Francia ha interpuesto una multa de 100.000€ a Google por la incorrecta aplicación del Derecho al Olvido. Esto es debido a que solamente eliminaba los datos de los buscadores de donde procedía la reclamación, considerando la Comisión que han

[87] RALUCA STROIE, I: "¿Es o no es google Spain responsable del tratamiento de datos personales?", *en Revista CESCO de derecho al consumo*, nº 17, 2016, p.1.

[88] RALUCA STROIE, I: "¿Es o no es google Spain responsable …ob cit., p.1.

de ser eliminados de todo el mundo y no solo en la extensión Francesa como es el caso[89].

7. Responsabilidad por la lesión del derecho al honor, intimidad personal y propia imagen en la red

Hasta finales del siglo XX la vulneración causada sobre los derechos de la personalidad se producían por medio de carteles, comunicados, etc., que se colocaban en lugares públicos, eran leídos ante una multitud de personas o emitidos por radio o televisión. Pero con la llegada de Internet, la expansión de las telecomunicaciones por medio de las redes y el intercambio de información a través de las mismas por cualquier persona desde cualquier lugar, amplio las posibilidades de vulneración de estos derechos dificultando la identificación y localización de sus responsables y por lo tanto la posibilidad de exigir responsabilidades.

La protección de los derechos de la personalidad establecidos en el art. 18 de la CE, concretan su protección en el art. 7 apartado 5 de la Ley Orgánica 1/1982, de 5 de mayo, en materia de protección civil del derecho al honor, intimidad personal y familiar y propia imagen, según el cual, se considerarán intromisiones ilegítimas "la captación, reproducción o publicación por fotografía, filme o cualquier otro procedimiento de la imagen de una persona en lugares o momentos de su vida privada o fuera de ellos, salvo los casos previstos en el art. 8.2", salvo cuando esté autorizado por ley o se hubiere otorgado el consentimiento expreso. Por lo tanto, nadie puede publicar una fotografía nuestra en redes sociales, o cualquier información, sin nuestro consentimiento expreso (con la salvedad de que sean personas de relevancia pública o la imagen sea tomada en un lugar público)[90].

En el supuesto de publicación de datos personales o fotografías sin un consentimiento expreso podremos acudir al gestor de la web o plataforma donde se haya publicado, o directamente ante los Tribunales a pedir responsabilidad. La protección de estos derechos puede darse por el orden civil, en la cual se exigirá la retirada de la información o imagen, y la solicitud para resarcir por los daños y perjuicios causados. Por otro lado, en el supuesto de que se haya injuriado o calumniado podremos acudir también a la vía penal.

En la actualidad, algunas empresas que explotan algunas redes sociales (Facebook, Twitter,…) introducen en sus determinados "términos o códigos de uso"[91] una declaración de derechos y responsabilidades para aquellos contenidos que estén protegidos por derechos de propiedad intelectual, de los que es dueño el usuario de la plataforma, y así que otorgue esté (usuario) a través de una aceptación de esos términos una licencia para que dicha empresa pueda

[89] JIMÉNEZ FERNÁNDEZ, V: "Multa de 100.00€ a google por la incorrecta aplicación del derecho al olvido", en *Centro de Estudios de Consumo*, 2016, pp. 1-2.

[90] En el supuesto de alguien publique nuestra dirección o cualquier hecho que no queramos divulgar es también protegible en virtud de lo dispuesto en dicha Ley Orgánica.

[91] TOMAS, I: *Protección del derecho a la intimidad y al honor en redes sociales y otras herramientas de internet*, ed Premium, Barcelona, 2015, p. 1.

utilizarlos. Pero, quien otorga ese consentimiento luego puede revocarlo, pudiendo retirar sus imágenes o información, pero ¿qué sucede en el caso de que esa imagen haya sido compartida por más usuarios o plataformas? En la STJUE (Gran Sala) de 13 de mayo de 2014 (TJCE 2014, 85)[92], se declara que cualquier persona puede dirigirse a las principales plataformas para solicitar la retirada de la información o fotografías, y por lo tanto, en el supuesto planteado, el responsable de la red social o plataforma está obligado a eliminarlo de forma total de toda la red.

También puede darse la situación de que alguien que no podemos identificar realice una publicación de una imagen o información sin nuestro consentimiento. Respecto a esto, la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSICE)[93], establece una responsabilidad de los prestadores de servicios de intermediación de la sociedad de información. Por lo que, en el caso de que esto suceda, debemos dirigirnos a los titulares de la red social o plataforma web, los cuales deben tomar precauciones, ya que no serán responsables en el supuesto de que no tuvieran conocimiento de que ese dato es ilícito o lesiona derechos o de saberlo no actúa con la diligencia debida y los retira.

Por lo tanto, la participación activa en las redes da lugar a un riesgo para el usuario, en el sentido de que se publiquen sus datos personales, pero además el riesgo de que él mismo publique datos de terceros sin el consentimiento de estos. La propia AEPD recomienda configurar adecuadamente el grado de privacidad de los perfiles (como podemos observar algunas plataformas como por ejemplo Facebook y WhatsApp, han configurado que los perfiles no sean completamente públicos, y que solo accedan al mismo los señalados como "amigos" por el usuario).

7.1 Las redes como responsables del tratamiento de datos personales

La AEPD en su Informe Jurídico 0197/2013 indica que "aquel que proporciona un servicio en la red social tendrá la condición de responsable del fichero" (definido además en el art. 3.d) de la LOPD)[94]. Este informe insiste en que la Directiva Europea de Protección de Datos (95/46/CE) (actualmente el nuevo Reglamento Europeo)[95] se aplica mayormente a los proveedores de las redes sociales, considerándoles por lo tanto responsables del tratamiento de los datos personales, ya que según estas, proporcionan los medios que permiten el tratamiento de los datos por los usuarios, así como los servicios básicos de gestión, por lo que estarán sujetos a todas las obligaciones y deberes impuestos por la LOPD.

[92] Caso Google Spain S.L Agencia Española de Protección de Datos (AEPD).

[93] BOE, núm.166, de 12 de julio de 2002.

[94] ÁLVAREZ, J: *Internet, redes sociales y protección de datos*, ed Aranzadi S.A, 2014, p. 3.

[95] Directiva 95/46/CE, de 24 de octubre de 1995, relativa a la protección de las personas físicas a lo que respecta al tratamiento de datos personales y la libre circulación de estos datos (DOCE L281 de 23 de noviembre de 1995), derogada actualmente por el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 (DOUE de 4 de mayo de 2016).

Pero existen diferencias legislativas en materia de protección de datos entre los países miembros de la UE, con los que son de los EE.UU, lo que crea grandes dificultades, sin embargo, por mandato de los arts. 2.1 de la LOPD y 3.1 del RLOPD, estarán obligados a cumplir la normativa europea (española si estuviera ubicada en España) los titulares de los servicios de las redes sociales que están ubicados en un Estado de la UE o utilizan medios de tratamiento situados en ella. En este sentido también se pronunció la AEPD en su Informe Jurídico 0454/2009 y el Grupo de Trabajo del art. 29[96].

Además, el Reglamento Europeo de Protección de Datos presentado por la Comisión el 25 de enero de 2012[97], implanta nuevas obligaciones del responsable del tratamiento de datos personales[98]. Pero respecto a la jurisdicción aplicable, a diferencia de lo que establecía la Directiva, éste tiene en cuenta la necesaria orientación hacia las personas, es decir, pretende aplicarse a los tratamientos de datos personales de interesados que residan en la UE por parte de un responsable que no esté ubicado en ella cuando sus actividades de tratamiento estén relacionas con la oferta de bienes y servicios dirigida a esos interesados en la UE. Asimismo, establece la obligación, aunque con excepciones[99], de estos responsables, que no se encuentran en la UE de designar un representante de ella al que poder dirigirse, por ejemplo en España es la AEPD.

Por lo tanto, estas normativas imponen a los proveedores de servicios de la red someterse a los dictados normativos Europeos en materia de protección de datos independientemente de donde esté situada su sede.

7.2 Los usuarios y su condición de responsables

Los usuarios de las plataformas virtuales tienen la condición general de afectados ya que son los titulares de los datos que son materia de tratamiento, así lo afirma el art. 3.e) de la LOPD: "afectado o interesado: persona física titular de los datos que sean objeto del tratamiento al que se refiere el apartado c) del presente artículo". Pero, los usuarios también son los usuarios los que incluyen datos personales o imágenes de otras personas en sus perfiles.

Normalmente, a las actividades que realizan los usuarios en dichas plataformas no se les puede aplicar la normativa de protección de datos, al ser actividades en el ámbito doméstico o privado según el art. 2.2.a) de

[96] Este grupo de trabajo es un órgano consultivo europeo independiente dedicado a la protección de datos y se creó en virtud del art. 29 de la Directiva 95/46/CE.

[97] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 (DOUE de 4 de mayo de 2016).

[98] Como la realización de una evaluación de impacto y el nombramiento de un delegado de protección de datos.

[99] En el supuesto en que esa entidad esté establecida en un país con un nivel adecuado de protección: cuando la empresa tenga menos de 250 trabajadores, cuando sea un organismo público, etc.

la LOPD ("A los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas") y el art. 4 de RLOPD, que precisa "siempre que no tenga un interés lucrativo". En el supuesto (y como advierte la AEPD en su informe 0197/2013) de que la utilización que se haga de las imágenes o datos, supere dicho ámbito de la vida privada o familiar, dará lugar automáticamente a la aplicación de la LOPD. Este podría ser el caso en el que se publiquen imágenes en una página de libre acceso, o cuando el elevado número de personas invitadas con dicha página resulte indicativo de que esa actividad se extiende más allá de lo que es propio en el ámbito doméstico o privado (siempre teniendo en cuenta el consentimiento del titular de los datos).

7.3 Responsabilidad civil

La actividad que realizan los administradores[100] de las redes sociales es legal, al igual que el acceso de los usuarios a las páginas web, pero la falta de control de los administradores de estas plataformas puede provocar que a través de estos medios se produzcan ilícitos, tanto penales como civiles. Por lo que en el caso de que no se imputara a dichos administradores la responsabilidad derivada del riesgo que asumen al crear tales plataformas, fundaría una sensación de que "en internet todo vale", cosa que sería muy perjudicial[101].

CARVALHO, en unos de sus artículos establece algunas teorías sobre cómo se podría razonar para hacer responsable a los administradores de las plataformas virtuales. Una de ellas sería la responsabilidad por hecho ajeno establecida en el art. 1903 del CC en el cual se menciona la responsabilidad por la realización de actos u omisiones por unos determinados sujetos (los padres, tutores, dueños o directores de centros,…). Pero, aunque no aparecieran textualmente los administradores de plataformas virtuales, podríamos interpretarlo como a título ejemplificativo, plasmando la realidad que existía en el momento de su creación, sin que pueda ser considerado como *numerus clausus*. De hecho, el Tribunal Supremo en la STS (Sala 1ª) de 23 de Septiembre de 1988 (RJ 1988, 6854) establece "que las normas deben de interpretarse conforme a la realidad social en la que se aplican velando por la seguridad jurídica de los ciudadanos"[102]. Pudiendo interpretar por lo tanto, que cabrían en este supuesto los administradores virtuales. Además podríamos realizar una interpretación analógica respecto del art. 4.1 CC, el cual establece: "procederá la aplicación analógica de las normas cuando éstas no contemplen un supuesto específico, pero regulen otro semejante entre los que se aprecia identidad de razón", por lo tanto, donde hay la misma razón, debe ser la misma disposición del Derecho, (principio *ubi eadem*

[100] Los administradores son aquellas personas que ostentan el dominio efectivo de la plataforma virtual.

[101] CARVALHO, A:"Redes sociales: responsabilidad de los administradores por la vulneración de derechos fundamentales", en *Aspectos profesionales: Protección de Datos, Cloud Computing y Sistemas de Gestión*, 2014, pp. 3-6.

[102] STS (Sala 1ª) 23 septiembre 1988 (FJ 3º), (RJ 1988,6854).

ratio ibique eadem legis dispositio[103]). Entonces los administradores de las plataformas virtuales serían responsables cuando conociendo que en su plataforma se ha producido la vulneración de los derechos fundamentales de un sujeto y no actúen con la diligencia debida o suficiente.

La protección civil de estos derechos está amparada en la Ley Orgánica 1/1982, de 5 de mayo, de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen[104], y está quedará supeditada por las leyes y los usos sociales atendiendo al ámbito que cada persona mantenga reservado para sí misma o su familia. Según ÁLVAREZ, se considerarán intromisiones ilegítimas en estos derechos en el ámbito de las redes sociales:

- "La divulgación en redes sociales hechos relativos a la vida privada de una persona o familia que afecten a su reputación y buen nombre, así como la revelación o publicación del contenido de cartas, memorias u otros escritos personales de carácter íntimo.
- La publicación en una red social de fotografías de una persona en lugares o momentos de su vida privada, sin su consentimiento.
- La imputación de hechos, o la manifestación de juicios de valor, a través de la publicación de comentarios en una red social, que lesionen la dignidad de otra persona, menoscabando su fama o atentando contra su propia imagen.
- La utilización de cualquier medio que permita acceder a los mensajes o contenidos privados de un usuario, así como su registro o reproducción"[105].

Respecto a las personas jurídicas a las cuales se haya visto afectado sus derechos de la personalidad de forma virtual, podría interponer la correspondiente acción de reclamación de daños y perjuicios[106] en defensa de sus intereses, teniendo en cuenta siempre el derecho de libertad de expresión.

Por otro lado, respecto a la responsabilidad civil derivada de infracción penal, la podemos encontrar en los arts. 109 a 115 y 116 a 122 del CP[107].

En primer lugar, el hecho de que se perpetre un delito a través de la Red por el usuario del servicio del que se deriven daños o perjuicios puede generar para el mismo responsabilidad civil como autor o como cómplice.

---

[103] El principio *"ubi eadem ratio ibique eadem legis dispositio"*, es un principio del derecho que significa que donde hay la misma razón, debe ser la misma disposición del Derecho, es decir, que los casos iguales deben ser tratados igualmente.

[104] BOE, núm. 115, de 14 de mayo de 1982.

[105] ÁLVAREZ, J*: Internet, redes sociales…* ob.cit.*,* p. 15.

[106] Conforme el art. 1101 CC, es aquella acción del perjudicado para exigir al causante del daño una cantidad de dinero equivalente a la reparación del mal causado.

[107] Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal (BOE, núm. 281, de 24 de noviembre de 1995).

En el caso de que el usuario sea menor de edad, pueden responder civilmente otros sujetos según lo establecido en el art. 61.3 de la LORPM[108], sin perjuicio de los demás supuestos de responsabilidad ajena por delitos perpetrados por el usuario previstos en los art. 61 a 63 LORPM. Este tipo de responsabilidad comprende tres modalidades (art. 110 CP):

- restitución de la cosa, se darían muy pocos casos en la práctica virtual, ya que se trata más bien para delitos patrimoniales.
- reparación del daño, que podrá consistir en obligaciones de dar, hacer o no hacer (esta si suele darse en la práctica virtual)
- indemnización de perjuicios materiales y morales, no solo para el agraviado, sino también para sus familiares o terceros. Esto supone para las redes sociales muchas posibilidades de reparación por múltiples conceptos con compleja cuantificación[109].

En segundo lugar, la perpetración de un delito a través de la Red por el prestador del servicio, cuando de él se deriven daños o perjuicios, puede generar también responsabilidad civil como autor o cómplice. Este sería el supuesto en el que este prestador o gestor del servicio, ante la perpetración de un delito a través de la red, se limite a una postura pasiva negligente, incumpliendo por lo tanto sus deberes legales (arts. 16 y 17 LSSICE[110]) por lo que podría responder civilmente según lo establecido en el art.120.3 CP, sin perjuicio, como ya comentaba anteriormente, de los supuestos de responsabilidad ajena (arts. 16 y 17 LORPM y 116 a 122 CP). Al igual que el anterior, comprende tres modalidades (restitución, reparación e indemnización). Como señala el Instituto Nacional de Ciberseguridad, y por la LSSICE, la responsabilidad de estos prestadores de servicios está delimitada, no teniendo sólo responsabilidad por las conductas realizadas directamente por ellos o por su personal, sino también por aquellas conductas de los usuarios de sus servicios que dañan la imagen o reputación de los terceros, aunque aquí existe una exención de responsabilidad, que consiste en la falta de obligación de su previsión o monitorización de los mensajes, datos o contenidos que circulan por su servicio o se alojan en él, y de los hiperenlaces que incluyen los usuarios, y la falta de responsabilidad por aquellos contenidos o hiperenlaces ilícitos siempre que no se tenga conocimiento efectivo de su existencia y actúen con la diligencia debida retirándolos en el momento de su conocimiento.

7.3.1 Valoración y cuantificación del daño moral por la lesión del derecho a la intimidad

[108] Ley Orgánica 5/2000, de 12 de enero, reguladora de la responsabilidad penal de los menores. (BOE, núm. 11, de 13 de enero de 2000).

[109] Se puede acudir a la posibilidad del art. 115 CP, estableciendo las bases en sentencia y fijando la cuantía en ejecución.

[110] Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (BOE, núm.166, de 12 de julio de 2002).

Podemos encontrar todo tipo de daños, ya sean, psíquicos, físicos y materiales que puedan resultar cuantificables y que responden a consecuencias resarcitorias de un acto discriminatorio al amparo de la Directiva de 2004 y la LOI, pero ¿Qué sucede con los daños morales puros?, es decir, de aquellos correspondientes a padecimientos como puede ser humillación, angustia, temor, etc., y que no comportan necesariamente una enfermedad psíquica. Estos daños son difícil de demostrar, por lo que es muy complicado probarlos. Pero la jurisprudencia ha encontrado la solución a través de "la Doctrina de la automaticidad de la indemnización" fundamentado en el gran valor que tiene el bien jurídico protegido.

La presunción de un daño moral que tiene su origen en el art. 9.3 de la LO 1/1982, de 5 de mayo, estableciendo que: "la existencia de un perjuicio se presumirá siempre que se acredite la lesión de un derecho de la personalidad". Por lo tanto, una vez reconocida la vulneración de un derecho fundamental, se determinará la indemnización en función del daño moral unido a la vulneración del Derecho Fundamental, como los daños y perjuicios adicionales derivados. Además, el art. 183 LRJS[111] ha consolidado la doctrina, admitiendo la indemnización adicional por daños y perjuicios[112]. Lo encontramos también la a Directiva 2006/54/CE, de 5 de julio (LCEur 2006, 1696), relativa a la aplicación del principio de igualdad de oportunidades e igualdad de trato entre hombres y mujeres en asuntos de empleo y ocupación[113], concretamente en su art. 18 que afirma que: "la indemnización de los perjuicios sufridos a causa de discriminación por razón de sexo debe configurarse con una finalidad disuasoria y proporcional al perjuicio sufrido".

La jurisprudencia de la Sala 1ª ha aplicado esta doctrina, cosa que no ocurrió en la jurisprudencia de la Sala.4ª[114]. Pero, tras la STC 24 de julio de 2006 (RTC 2006, 247)[115], hay un cambio, aunque se

[111] Ley 36/2011, de 10 de octubre, reguladora de la jurisdicción social (BOE, núm. 245, de 11 de octubre de 2011).

[112] En efecto, este mismo artículo en su apartado 2, concreta los objetivos de dicha indemnización, afirmando que no se limitan a "resarcir suficientemente a la víctima y restablecer a ésta, en la medida de lo posible, en la integridad de su situación anterior a la lesión", sino que la compensación económica debe "contribuir a la finalidad de prevenir el daño".

[113] DOUE, núm.204, de 26 de julio de 2006.

[114] Por ejemplo, la STS (Sala 4ª) de 22 de julio de 1996 (RJ 1996, 6281). Asimismo, en el mismo sentido, vid. STS (Sala 4ª) de 30 de enero de 1997 (RJ 1997, 647).

[115] A este respecto, vid. la STS (Sala 4ª) de 5 de febrero de 2013 (RJ 2013, 3368), según la cual "la cuantificación del daño moral derivado de la conducta infractora puede basarse en las propias características de esta última (gravedad, reiteración y otras circunstancias concurrentes), utilizando como elemento delimitador el importe de la sanción establecida para la infracción en la LISOS". (Ley sobre infracciones y sanciones del orden social). Del mismo modo, vid. SSTS (Sala 4ª) de 25 de enero de 2010 (RJ 2010, 3125) y de 11 de enero de 2015 (RJ 2015, 1011). También SSAN (Sala 4ª) de 27 de julio de 2012 (AS 2012, 2512) y de 13 de julio de 2012 (AS 2012, 2582), entre otras.

admite y reconoce la existencia de un daño moral consecuencia de la lesión de un derecho fundamental, se exige probar la existencia de un indicio moral[116]. Se requiere que el daño moral sea alegado en el proceso, precisando su alcance y acreditarlo, salvo que exista una "implicación directa" entre la conducta lesiva y la vulneración del derecho fundamental, como sucede con el derecho al honor. Pero, está limitación resulta justificada en los casos que se atente sobre la libertad sindical.

También encontramos como relevante el art. 25.1 del Proyecto de Ley de Igualdad de trato y no discriminación[117], el cual establece que: "la persona que cause discriminación por alguno de los motivos previstos en el apartado primero del artículo de esta Ley responderá del daño causado. Acreditada la discriminación se presumirá la existencia de daño moral, que se valorará atendiendo a las circunstancias del caso y a la gravedad de la lesión efectivamente producida, para lo que se tendrá en cuenta, en su caso, la difusión o audiencia del medio a través del que se haya producido". Por ello, es lógico presumir la existencia de ese daño moral una vez acreditada la vulneración del derecho fundamental, pero si es posible establecer criterios que partan de la gravedad de esa vulneración. Aunque los tribunales atiendan a la gravedad de la vulneración, no existe homogeneidad, por lo que resulta de aplicación el baremo circulatorio de forma orientativa.

En efecto, la dificultad que a efectos de cuantificación de estos daños puede advertirse, permite que los Tribunales se basen, por regla general y con carácter orientativo y no vinculante fuera del ámbito circulatorio, en esta sede, en el baremo derivado del Texto Refundido de la Ley sobre Responsabilidad Civil y Seguro de Circulación de Vehículos a Motor, por Real Decreto Legislativo 8/2004, de 29 de octubre[118], ha sido objeto de una relevante modificación por la Ley 35/2015, de 22 de septiembre, de reforma del sistema para la valoración de los daños y perjuicios causados a las personas en accidentes de circulación[119].

7.4 Responsabilidad penal

Se encuentra establecida en los arts. 11, 27, 28, 29, 31 y 31 bis del Código Penal en materia de comisión por omisión y las personas criminalmente responsables (sin perjuicio de lo establecido en los arts. 32 y 108 del mismo Código sobre clasificación, aplicación, efectividad, sustitución de las penas y medidas de seguridad) y en la Ley Orgánica 1/2015, de 30 de

[116] Entre otras, vid. STS (Sala 4ª) 12 diciembre 2007 (RJ 2008, 3018).

[117] BOCG, 10 de junio de 2011.

[118] BOE, núm. 267, de 5 de noviembre de 2004.

[119] BOE, núm. 228, de 23 de septiembre de 2015.

marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal (derogación del Libro III, faltas y sus penas)[120].

Por un lado, la comisión de un delito a través de la red por un usuario (destinatario del servicio) puede producir responsabilidad penal como autor o cómplice, de conformidad con los arts. 11 y 27 a 31 quinquies del CP. De forma general, los autores de los delitos, teniendo en cuenta el carácter parcialmente cerrado de las plataformas (ya que se necesita el registro) son los usuarios, pero también pueden ser terceros o incluso el propio prestador del servicio. Los usuarios pueden participar de forma activa en las plataformas, lo que implica haber aceptado con ocasión del registro las condiciones del prestador del servicio. En la práctica, la no existencia de sistemas de control previo (ya sea en los registros, como en los contenidos), permite que se den conductas ilícitas muy variadas, tanto por los usuarios (revelación de secretos, injurias, amenazas, etc.) como por los terceros que acceden a este tipo de plataformas. Generalmente, este tipo de responsabilidad implica a quien comete directamente el hecho principal, pero también puede implicar a otros sujetos en algunos casos.

Por otro lado, en el supuesto de la perpetración de un delito a través de la red por el prestador del servicio, de igual forma puede generar para el mismo responsabilidad penal como autor o cómplice, de conformidad con lo establecido en el art. 11 y 27 a 31 quinquies del CP. Este tipo de responsabilidad está delimitada por la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI), que traspone a la Directiva 2000/31/CE de Comercio Electrónico[121], la cual establece que los proveedores son responsables en todos los órdenes (ya sea penal, civil o administrativo), de aquellas conductas consumadas por ellos o por el personal a su servicio y que impacten en los derechos de los usuarios. No obstante, respecto a las conductas de los usuarios de sus servicios que dañan la reputación o imagen de terceros, los arts. 16 y 17 de LSSI, parten de unos principios básicos que determinan una exención de responsabilidad:

- Que el prestador del servicio no tiene obligación alguna de supervisión o monitorización de los mensajes o contenido que se alojan o que circulan por su servicio, ni de los hiperenlaces[122] que incluyen los usuarios.
- Que el prestador del servicio no responde de contenidos o hiperenlaces ilícitos siempre que no tenga conocimiento efectivo[123]

[120] BOE, núm. 281, de 24 de noviembre de 1995.

[121] Directiva 200/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (DOUE, núm. 178, de 17 de julio de 2000).

[122] Es un hipervínculo o enlace que de ser pulsado te lleva a la apertura de otra página web o archivo.

[123] El conocimiento efectivo se produce cuando un órgano competente declara la ilicitud de los datos, ordenando su retirada o que se imposibilite el acceso a los mismos, o cuando se declaré la existencia de

de su existencia, y en caso de tenerlo, actúe con diligencia retirándolos o haciendo imposible el acceso.

Por lo tanto, el prestador del servicio podrá incurrir en responsabilidad penal en el caso de adoptar una actitud activa por el alojamiento de contenidos o facilitación de enlaces ilícitos o lesivos que proporciona un usuario que actúa bajo su dirección o control. Pero también incurriría en este tipo de responsabilidad en el supuesto de adoptar una postura pasiva por la falta de retirada o de impedimento de acceso a este tipo de contenidos ilícitos o lesivos.

8. **Conclusiones**

1. En la actualidad, está cambiando el significado de términos como el de intimidad o propia imagen. Las redes sociales e Internet se han convertido, para muchos, en un diario en directo de todo lo que sucede en sus vidas, publicando lo que se hace, lo que se piensa, donde vamos, con quien, etc. Pero además, se publican indiscriminadamente imágenes propias y ajenas. Se va devaluando poco a poco el significado de la intimidad y se acepta con total normalidad que se cuelguen imágenes de cualquiera sin contar con su consentimiento ni el de sus padres (en el caso de menores). El valor que tiene la información no puede cuestionarse, la información es poder, que puede utilizarse con fines beneficiosos para la sociedad o de forma perjudicial.
2. La violación sistemática de los derechos de la personalidad que se manifiesta a través de las redes sociales, no es un tema baladí. No podemos olvidar que estamos ante derechos fundamentales por lo que las leyes deberían de ser más eficaces no ya solamente en su protección, sino en lo que se refiere a la posibilidad de restablecernos y resarcirnos nuestro derecho una vez que denunciamos la aparición, por ejemplo, de nuestra imagen no consentida en la red. Es necesario articular normas y sistemas eficaces que posibiliten el borrado total de los datos personales o una fotografía cuando así lo exija la persona que en ella aparece, tanto si no consintió en que se difundiera, como si lo consintió y hoy quiere revocar ese consentimiento.
3. Aunque sea cierto que las redes cuentan con nuestro consentimiento para tratar nuestros datos personales desde el momento en que nos abrimos una cuenta, y que nuestra potestad contra sus reglas o sobre cómo se aplican pueda ser consideradas no válidas por nuestra previa aceptación, debemos seguir insistiendo para que se produzca un cambio y las normas se acaben modificando para conseguir que nuestro consentimiento sea válido y conscientemente prestado.
4. El contrato que se establece entre el servicio web y el usuario está constituido, básicamente, por la cesión de sus datos personales e información al servicio, siendo ésta en muchas ocasiones privada, por lo que el servicio web está contractualmente obligado a proteger esa privacidad frente a cualquier intromisión que pueda dañar los derechos fundamentales del usuario. Por lo tanto, estos servicios deben asumir el deber contractual de proporcionar a sus

lesión, y el prestador tenga conocimiento de la resolución. Esto sin perjuicio de que se dé un conocimiento por parte del perjudicado a través de una notificación y el proveedor por tanto sea consciente de la ilicitud.

clientes una tecnología eficaz y precisa, detectando aquellos contenidos ofensivos, informando sobre ellos a quien les afecte y por supuesto, brindar soluciones. En el caso de no ser así, y a pesar del gran debate doctrinal que encontramos en la actualidad, el servicio web debería estar sometido a responsabilidad contractual frente al usuario que se ha visto afectado, resarciendo al mismo en la medida de lo posible.

5. Es cierto que el factor tiempo juega un papel indispensable y relevante en esta materia, ya que el Derecho siempre va a ser más lento que el avance tecnológico, deberíamos esforzarnos porque la tecnología y Derecho logren algún día ir a la par, para que el Derecho no pierda su sentido.
6. El desafío de la actualidad es lograr un marco regulador de la privacidad adecuado que consiga un efectivo equilibrio entre los intereses en juego, entre los intereses económicos de las empresas, la innovación y el crecimiento, la libertad de expresión e información, los intereses de los ciudadanos a la salvaguarda de su privacidad y derechos fundamentales. Pero además, desde mi humilde opinión, considero que sería necesaria la creación de un marco internacional unificado, ya que lo que creo que supone más problemas a la hora de defender nuestros derechos fundamentales, es la escasez de normativa internacional, teniendo en cuenta que la gran parte de las empresas virtuales tienen su sede principal fuera de Europa.

9. Bibliografía

A) Libros, artículos y capítulos

- ÁLVAREZ CARO, M: *Derecho al olvido en Internet: El nuevo paradigma de la privacidad en la era digital,* ed: Reus S.A, Madrid, 2015, pp. 1-144.
- ÁLVAREZ, J: "Internet, redes sociales y protección de datos", *Aranzadi, SA*, 2014, pp. 1-652.
- APARICIO, J: *Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal*, 3ª Edición, ed. Aranzadi-Thomson Reuters, 2009, pp. 1-464.
- CARVALHO, A: Redes sociales: responsabilidad de los administradores por la vulneración de derechos fundamentales, en *Aspectos profesionales: Protección de Datos, Cloud Computing y Sistemas de Gestión*, 2014, p.1.
- CEREZO GILARRANZ, J: "Presentación. Identidad digital y reputación online", en *Cuadernos de comunicación Evoca. Evoca Comunicación e Imagen,* 2011, pp. 1-50.
- CHINCHILLA SANDÍ, C: "Personalidad virtual: necesidad de una reforma constitucional", en *Revista de Derecho y Tecnologías de la información*, 3, 2005, pp. 1-11.
- CORREDOIRA, L; COTINO, L: *Libertad de expresión e información en Internet: amenazas y protección de los derechos personales*, ed: Centro de Estudios Políticos y Constitucionales, Madrid, 2013, pp. 1-541.
- FAERMAN, J: *Faceboom, el nuevo fenómeno de masas*, Alienta Editorial, Barcelona, 2010, pp. 1-160.
- GARCÍA ESTÉVEZ, N: *Redes sociales en Internet. Implicaciones y consecuencias de las plataformas 2.0 en la sociedad*, editorial Universitas, Madrid, 2012, pp. 1-342.

- GARCÍA, L: "¿Utiliza Facebook nuestros datos personales?", en *Centro de Estudios de Consumo*, 2016, pp. 1-7.
- HOLAND, B: "Privacy Paradox 2.0", en *Widener Law Journal*, Vol. 19, nº3, 2010, pp. 1-41.
- JIMÉNEZ, V: "Multa de 100.00€ a google por la incorrecta aplicación del derecho al olvido", en *Centro de Estudios de Consumo*, 2016, pp. 1-2.
- LAWRENCE, L: *Digital Law World Congress: On the future of IP Law*, Barcelona, 2012, p.1.
- LESMES SERRANO, C*: La Ley de Protección de Datos. Análisis y comentario de su jurisprudencia,* Lex Nova, Valladolid, 2008, pp. 1-12.
- LIZARRA VIZCARRA, I: *El derecho de rectificación*, ed Aranzadi. Cizur Menor, Navarra, 2005, pp. 1-172.
- LÓPEZ, E: *El derecho al honor y el derecho a la intimidad*, ed Dykinson, Madrid, 1996, pp. 1-245.
- MAYER-SCHÖNBERGER, V; CUKIER, K: *Big Data: la revolución de los datos masivos*, Editorial Turner Noema, Madrid, 2013, pp. 1-143.
- NAVAS, S: *La personalidad virtual del usuario de internet: Tratamiento de la información personal recogida mediante cookies y tecnología análoga*, ed: Tirant lo Blanch, Madrid, 2014, pp. 1-294.
- PEREZ, P; GUTIERREZ, C; DE LA FUENTE, S; GARCÍA, L; ALVAREZ, E: *Guía de Introducción a la Web 2.0: aspectos de privacidad y seguridad en las plataformas colaborativas*. Instituto Nacional de Tecnologías de la Comunicación, 2011, pp. 1-33.
- PEREZ ROYO, J: *Curso de Derecho Constitucional*, ed Marcial Pons, Madrid, 2010, pp. 1-901.
- PONCE, I: *Redes Sociales*. Instituto de Tecnologías de la Comunicación, 2012, p.1.
- QUESADA, A: *Protección de datos y telecomunicaciones convergentes,* Agencia Española de Protección de Datos, Madrid, 2015, pp. 1-470.
- RALLO, A; MARTÍNEZ, R: *Derecho y redes sociales 2ª Edición,* ed: Thomson Reuters, 2013, pp. 1-562.
- RALUCA, I: "¿Es o no es google Spain responsable del tratamiento de datos personales?", en *Revista CESCO de derecho al consumo,* nº 17, 2016, pp. 1-6.
- ROMERO, P: "La engañosa privacidad de las fotos de Facebook", en *El Mundo*, 2011, p.1.
- SALVADOR CODERCH, P: "Imágenes veladas. Libertad de información, derecho a la propia imagen y autocensura de los medios", en *InDret*, nº 1, 2011, pp. 1-51.
- TESONE, R: "Los retos de la privacidad: innovación, derecho y seguridad", en *CEU*, Madrid, 2014, p.1.
- TOMAS, I: *Protección del derecho a la intimidad y al honor en redes sociales y otras herramientas de internet*, ed: Premium, Barcelona, 2015, p.1.
- TRONCOSO REIGADA, A: "Las redes sociales y la APDCM", en *Datos personales*, nº43, 2010, p.1.

B) Páginas web

- ARRINGTON, M: "Facebook's Zuckerberg Says The Age of Privacy is Over", en *Techcrunch,* 2010, p.1: http//www.readwriteweb.com/archives//Facebook_zuckerberg_says_the _age_of_privacy_is_ov.php (Consultado 13/05/2016).
- CARRIÓN, H: *La sociedad de la información. Tecnologías de información y telecomunicaciones*, Centro de Investigación para la Sociedad de la Información, 2013, pp. 1-166: http://www.imaginar.org/docs/sociedad_información_wikipedia.pdf (Consultado 10/05/2016).
- GUADAMUZ, A: "Habeas Data: The Latin American Response to Data Protection. Warwick website", en *Electronic Law Journals,* 2000, p.1: http://elj.warwick.ac.uk/jilt/00-2/guadamuz.html. (Consultado 03/03/2016).
- KIRSH, E; PHILIPS, D; MCINTYRE, D: "Recommendations for the Evolution of Cyberlaw", en *Journal of Computer-Mediated Communication,* Indiana, 1996, pp.1-85: www.jcmc.indiana.edu/vol2/issue2/jcmc223.htm. (Consultado 03/03/2016).
- LEINER, B; CERF, V; CLARK, D; KAHN, R; KLEINROCK, L; LYNCH, D; WOLFF, S: *A brief history of the Internet,* Universidad de California, Santa Bárbara, 2009, pp. 1-10: http://www.cs.ucsb.edu/almeroth/classes/F10.176A/papers/internet-history-09.pdf (Consultado 02/03/2016).
- MORALES VIALES, R Y UGARTE IBARRA, R: *Tutela de los derechos de la personalidad virtual y protección de datos de carácter personal en las redes sociales on line*, Instituto de Investigaciones Jurídicas de la Universidad de Costa Rica, 2012, pp. 1-190: www.iij.ucr.ac.cr/download/file/fid/627 (Consultado 12/04/2016).
- SUÑE, E: *Del derecho informático al derecho del ciberespacio y a la constitución del ciberespacio*, Iuris Tantum vLex, 2006, p. 1: http://doctrina.vlex.com.mx/vid/informatico-ciberespacio-54803677 (Consultado 07/04/2016).

ÍNDICE JURISPRUDENCIAL

STJUE (Gran Sala) de 13 de mayo de 2014 (TJCE 2014, 85).
STC (Sala 2ª) de 25 de abril de 1994 (RTC 1994,117).
STC (Pleno) de 30 de noviembre de 2000 (RTC 292, 2000).
STC (Pleno) de 30 de noviembre de 2000 (RTC 290, 2000).
STC (Sala 1ª) de 30 de junio de 2003 (RTC 2003,127).
STC (Sala 1ª) de 15 de noviembre de 2004 (RTC 2004,196).
STC (Sala 1ª) de 3 de julio de 2006 (RTC 2006, 196).
STC (Sala 1ª) de 15 de enero 2007, (RTC 2007, 9).
STC (Sala 1ª) de 24 de septiembre de 2007 (RTC 2007, 206).
STC (Sala 2ª) de 26 de enero de 2009 (RTC 2009, 29).
STC (Sala 1ª) de 23 de marzo de 2009 (RTC 2009, 77).
STC (Sala 1ª) de 27 de abril de 2010 (RTC 2010,23).
STC (Sala 1ª) de 11 de abril de 2011 (RTC 2011, 41).
STC (Pleno) de 9 de mayo de 2013 (RTC 2013, 115).
STS (Sala 1ª) 23 septiembre 1988 (RJ 1988,6854).

STS (Sala 4ª) de 22 de julio de 1996 (RJ 1996, 6381).
STS (Sala 4ª) de 30 de enero de 1997 (RJ 1997, 647).
STS (Sala 4ª) 12 diciembre 2007 (RJ 2008, 3018).
STS (Sala 1ª) de7 de noviembre de 2008 (RJ 2008, 5903).
STS (Sala 1ª) de 5 de mayo de 2009 (RJ 2009, 147).
STS (Sala 4ª) de 25 de enero de 2010 (RJ 2010, 3125).
STS (Sala 4ª) de 5 de febrero de 2013 (RJ 2013, 3368).
STS (Sala 4ª) de 11 de enero de 2015 (RJ 2015, 1011).
STS (Sala 3ª) de 15 de marzo de 2016 (RJ 2016, 1301).
SAN (Pleno) de 27 de abril de 2006 (RTC 132, 20069).
SAN (Sala 1º), de 18 de mayo de 2006 (530,2004).
SAN (Sala 4ª) de 13 de julio de 2012 (AS 2012, 2582).
SAN (Sala 4ª) de 27 de julio de 2012 (AS 2012, 2512).

ABREVIATURAS Y SIGLAS

AEPD	Agencia Española de Protección de Datos
APEC	Asia-Pacific Economic cooperation (Foro de cooperación económica Asía- Pacífico
ARCO	Acceso, rectificación, cancelación y oposición
ARPANET	Advanced Research Projects Agency Network (La Red de la Agencia de Proyectos de Investigación Avanzada)
art.	Artículo
arts.	Artículos
CC	Código Civil
CE	Constitución Española
CP	Código Penal
DNI	Documento Nacional de Identidad
EE.UU	Estados Unidos
ENISA	European Network Information Security Agency (Agencia de Seguridad en las redes de la Información Europea)
Etc	Etcétera
FJ	Fundamento Jurídico
INC	Incorporated (Incorporación)

IWGDPT	International Working Group on Data Protection and Telecomunications (Grupo de trabajo internacional sobre la protección de datos en telecomunicaciones)
LEC	Ley de Enjuiciamiento Civil
LISOS	Ley sobre Infracciones y Sanciones del Orden Social
LOPD	Ley Orgánica sobre Protección de Datos
LOPDCP	Ley Orgánica sobre Protección de Datos de Carácter Personal
LORPM	Ley Orgánica de Responsabilidad Penal de Menores
LSSICE	Ley de Servicios de la Sociedad de Información y de Comercio Electrónico
núm.	Número
ob.cit.	Obra citada
OCDE	Organización para la Cooperación y el Desarrollo Económicos
OTAN	Organización del Tratado del Atlántico Norte
p.	Página
pp.	Páginas
RJ	Repertorio Jurisprudencial
RLOPD	Reglamento de la Ley Orgánica de Protección de Datos de Carácter Personal
RTC	Repertorio del Tribunal Constitucional
SAN	Sentencia de la Audiencia Nacional
SSAN	Sentencias Audiencia Nacional
SSTC	Sentencias del Tribunal Constitucional
SSTS	Sentencias del Tribunal Supremo
STC	Sentencia del Tribunal Constitucional
STJUE	Sentencia del Tribunal de Justicia de la Unión Europea
STS	Sentencia del Tribunal Supremo

TIC	Tecnologías de la Información y de la Comunicación
TS	Tribunal Supremo
UE	Unión Europea
Vid.	Véase
Vól.	Volumen