APROXIMACIÓN AL RÉGIMEN JURÍDICO DE LAS REDES SOCIALES

JOSÉ MIGUEL BELTRÁN CASTELLANOS
Becario de Investigación del Área de Derecho Administrativo de la Universidad de Alicante

Recibido 25.03.2014 / Aceptado 03.06.2014

RESUMEN: Cada vez más gente emplea las redes sociales para compartir su información personal, experiencias, fotografías, proponer temas de debate, hacer amistades o reencontrarse con antiguos conocidos. Sin embargo, los usuarios de este tipo de plataformas muchas veces no saben qué sucede con la información que suben a la red, quién tiene acceso a la misma, si cuando se dan de baja esa información es borrada de los servidores o qué derechos amparan la privacidad de sus datos. Se elabora aquí un estudio aproximado de la regulación jurídica que protege a los usuarios, que obliga a los prestadores de los servicios a garantizar nuestra privacidad en la red y que impide que los menores de determinada edad empleen estas plataformas. Asimismo, se analizan cuáles son los problemas que plantea el uso de las redes sociales y cómo las recomendaciones y normas que vayan apareciendo en el futuro podrían aportar soluciones para hacer este medio de comunicación fácil de usar, transparente y seguro.
PALABRAS CLAVE: internet, redes sociales, privacidad, menores, consentimiento, derecho al olvido.

ABSTRACT: Nowadays it is very common for people to use social networks to share their personal information, experiences, hotographs, to propose debate issues, to make friends or to meet again with old partners. However, the users of these kinds of platforms sometimes do not know what happens with the information they upload to these networks, who is able to access it, if the information is deleted from the servers when the user deletes himself or which rights protects their data privacy. The article developes an approximate study about the legal regulation which protects users and forces the providers of the services to guarantee our privacy on the network and also not to allow children to use this platforms. Likewise, two matters have been analysed, the

problems does the use of the social network cause and what the suggestions and rules will appear in the future could bring solutions for finding the use of this mass media easy, clear and safe.

KEY WORDS: internet, social networks, privacy, children, consent, the right to forget.

SUMARIO: 1. INTRODUCCIÓN. 2. ¿QUÉ ES UNA RED SOCIAL? 3. CARACTERES Y ELEMENTOS DE LAS REDES SOCIALES. DESAFÍOS JURÍDICOS QUE PLANTEAN. 4. NORMATIVA Y ÁMBITO DE APLICACIÓN. 4.1. Servicios de la Sociedad de la Información. 4.2. Protección de Datos Personales. 4.3. Protección de la Privacidad, Honor, Intimidad y Propia Imagen. 4.4. Protección de Consumidores y Usuarios. 4.5. Protección de menores e incapaces. 5 PRINCIPIOS REGULADORES RECOMENDADOS POR LA COMISIÓN EUROPEA. 6. EL CONSENTIMIENTO EN LAS REDES SOCIALES. 7. DERECHO AL OLVIDO. 8. ANÁLISIS DE UNA RED SOCIAL: FACEBOOK. 9. CONCLUSIONES. 10. BIBLIOGRAFÍA.

1. INTRODUCCIÓN

Con el paso del tiempo, las comunicaciones personales en la Red han ido evolucionado, desde los tradicionales programas de mensajería instantánea como *Messenger*, hasta el concepto actual de *red social*, donde los usuarios ponen en común aficiones, gustos y vivencias con la única finalidad de que toda su red de contactos, que se encuentra en constante crecimiento, tenga acceso a dicha información. La red social en Internet supone una nueva forma de relación humana que se ha ido posicionando como uno de los medios de comunicación online más populares en la Red.

A pesar de las cifras de usuarios y los beneficios que puede suponer su uso, no se trata de un medio exento de posibles peligros, por lo que se hace preciso el crecimiento ordenado y adecuado de la legislación vigente. Especial trascendencia supone el hecho de que los menores de edad sean los principales usuarios de este tipo de plataformas. Dadas las características propias de los menores y su posición inicial de mayor indefensión, las instituciones públicas y la legislación vigente les han otorgado un mayor grado de protección, en aras de evitar, o al menos reducir, los efectos negativos derivados del uso de estas plataformas.

2. ¿QUÉ ES UNA RED SOCIAL?

Como concepto de red social, se puede afirmar que se trata de una aplicación online que permite a los usuarios, de forma completamente descentralizada, generar un perfil público, compartir información, colaborar en la generación de contenidos y participar de forma espontánea en movimientos sociales y corrientes de opinión[1].

Abordando una definición[2], las redes sociales son aquellos servicios de la sociedad de la información que ofrecen a los usuarios una plataforma de comunicación a través de internet para que éstos generen un perfil con sus datos personales, facilitando la creación de redes en base a criterios comunes y permitiendo la conexión con otros usuarios y su integración[3].

Por tanto, los usuarios de los servicios *on-line* acceden a la red social con el objetivo de comunicarse con otros usuarios, hacer amistades y compartir información entre la que se incluye fotografías y vídeos. Esas relaciones pueden tener distinto alcance. Así, en primer lugar, el usuario se comunica con sus contactos o amigos de forma directa, en segundo lugar, esa información será accesible por regla general a los contactos de sus contactos y, en tercer lugar, habrá información que sea accesible para todos los usuarios de la red social e incluso para cualquiera navegue por internet[4].

De este modo y a título de ejemplo, si introducimos en Google el nombre y apellidos de una persona registrada en Facebook (datos que suelen hacer de *usuario* en dicha red social[5]) nos aparecerá la pantalla de inicio de esta persona en esta red social con algunos datos más como su fecha de nacimiento y aficiones así como una fotografía, dándonos la opción de registrarnos si aún no lo hemos hecho y de agregarla como amigo/a.

---

[1] OBSERVATORIO DE LA SEGURIDAD DE LA INFORMACIÓN, *Redes Sociales, Menores de Edad y privacidad en la Red*, INTECO (Instituto Nacional de Tecnologías de la comunicación), 2007, p. 3, www.inteco.es.

[2] Art. 1, apartado 2, de la Directiva 98/34/CE, modificada por la Directiva 98/48/CE y transpuesta mediante la Directiva 2000/31/CE de comercio electrónico en la Ley 34/2002 de Servicios de la Sociedad de la Información y de Comercio Electrónico.

[3] RALLO LOMBARTE, A. Y MARTÍNEZ MARTÍNEZ, R. (Coord.), *Derecho y Redes Sociales*, Pamplona (Navarra), 2010, p. 24.

[4] El acceso a los perfiles de otros usuarios en una red social, depende de la configuración de la privacidad que cada uno aplique, así, por defecto, los perfiles están configurados "en abierto" y cada usuario puede ver toda información de ese perfil, incluyendo sus fotos y datos personales.

[5] En las redes sociales los usuarios suelen emplear, por regla general, sus nombres y apellidos para hacer "login" en su cuentas con el objeto facilitar a futuros contactos que los localicen y agreguen como amigos, lo que sería más complicado si se emplea en el registro un pseudónimo o apodo.

Por otro lado, el acceso a las redes sociales se ha intensificado con la expansión de las redes *wifi* y *3G*, de tal forma que haciendo uso de un ordenador portátil, un *Tablet* o un *Smartphone* los usuarios se encuentran prácticamente conectados durante casi la totalidad del día. De hecho, muchos reconocen conectarse a las redes sociales en la primera hora de la mañana.

No podemos concluir este apartado sin hacer mención de una nueva función que inunda las redes sociales, la comercial. Actualmente la práctica totalidad de las empresas disponen de perfiles en las redes sociales más comunes con el fin de hacer llegar sus productos a los potenciales clientes que conforman esta nueva "sociedad". Algunos empresarios incluso emplean estas plataformas para ofrecer puestos de trabajo o para saber si sus nuevos productos tendrán una buena acogida entre el público consumidor[6].

3. CARACTERES Y ELEMENTOS DE LAS REDES SOCIALES. DESAFÍOS JURÍDICOS QUE PLANTEAN

Existen una serie de elementos básicos o caracteres[7] que se dan en todas las redes sociales. De este modo, en primer lugar, tienen como finalidad principal poner en contacto a personas, de forma rápida, sencilla y, al menos en teoría, segura. Además, permiten la interacción entre todos los usuarios de la red social en cuestión, facilitando el intercambio de fotografías, vídeos e información de todo tipo, así como nuevos contactos.

En segundo lugar, favorecen la posibilidad de que usuarios de la plataforma acaben entablando un contacto real, es decir, físico y por tanto más allá del espacio *on line y* permiten que el contacto entre usuarios sea ilimitado, lo que supone que desaparecen las barreras geográficas y temporales. De hecho, es posible comunicarse

[6] La Red Social "Linkedin" está enfocada a las relaciones entre profesionales, fomentando la posibilidad de encontrar trabajo o nuevas oportunidades comerciales entre los usuarios que se unen a sus filas. https://es.linkedin.com

[7] OBSERVATORIO DE LA SEGURIDAD DE LA INFORMACIÓN, *Redes Sociales, Menores de Edad y privacidad en la Red*, INTECO (Instituto Nacional de Tecnologías de la comunicación), 2007, p. 3, www.inteco.es.

desde cualquier lugar y en cualquier momento, basta con disponer de una conexión a internet y de un ordenador personal o similares[8].

En tercer lugar, destacar el alcance o lo que se denomina, la difusión viral de la red social[9], ya que los contactos se comunican con los contactos de sus contactos, expandiéndose así el fenómeno "red social" de forma casi ilimitada, por toda la plataforma.

Sin embargo, no todo son bondades y dada la entidad, tamaño e incidencia que están tomando las redes sociales, existen gran cantidad de acciones y actos que las diferentes plataformas están realizando sin conocer o al menos sin cumplir principios básicos de la normativa española de protección de datos de carácter personal, de protección de la intimidad, la publicidad y la protección de la propiedad intelectual e industrial respecto a los contenidos creados y alojados por los usuarios en sus perfiles de usuarios.

Los principales problemas que se pueden identificar son[10]:

En primer lugar, compelen al usuario a facilitar un gran número de datos. Existe un problema derivado de la falta de conciencia por parte de los usuarios de la información que hacen pública en la red. Se trata de datos personales que en ningún caso expondrían en la vida offline, relativos a su ideología política y religiosa, orientación sexual, datos sobre su economía etc. Estos datos, que son los más próximos al núcleo de individualidad de la persona, la legislación española los ha llamado *datos esencialmente protegidos* [11] Hay que tener presente que las preferencias que se establecen por defecto en la plataforma son las menos protectoras para la privacidad.

En segundo lugar, los datos publicados pueden ser empleados por terceros de forma ilícita; se dan a conocer horarios en los que se encuentra una persona en su

[8] Como ya hemos mencionado, es posible y además se emplea frecuentemente, el uso de ordenadores portátiles, Tablets y Smartphones para acceder a las redes sociales, por lo que no es necesario encontrarse en casa o en el trabajo para hacer uso de las mismas.

[9] Las Redes Sociales pueden ser comparadas con un virus puesto que su finalidad principal es extenderse en la red, ampliando cada vez más su número de miembros. De esta forma, cada contacto invita a otros amigos a formar parte de la misma red social y así logra extenderse, hacerse popular e interconectar al mayor número posible de personas.

[10] RALLO LOMBARTE, A. Y MARTÍNEZ MARTÍNEZ, R. (Coord.), *Derecho y Redes Sociales*, Pamplona (Navarra), 2010, pp. 33 - 36.

[11] Así se calificaron en el artículo 7 de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal (Vigente hasta el 14 de enero de 2000).

domicilio, dónde aparca su vehículo, marca y modelo del mismo, nivel económico, segundas viviendas, colegio al que acuden los hijos, lugar de veraneo… Además puede darse el caso de que se publique en la Red información falsa o sin nuestra autorización, generando situaciones jurídicas perseguibles como delito de injurias e incluso calumnias. Finalmente se configura un entorno donde fácilmente puede producirse la suplantación de identidad.

En tercer lugar, existen riesgos que afectan al mayor sector de usuarios de las redes sociales, los menores de edad. Dado que no han alcanzado el grado de madurez suficiente se requiere una protección especial. No se trata de una cuestión baladí, puesto que son muchos los que "suben" a internet fotografías poco decorosas e interactúan con contenidos inapropiados para su edad. Además, su capacidad legal para otorgar su consentimiento en relación con la información que estas redes requieren resulta insuficiente y debe ser completada con el consentimiento de sus padres o tutores.[12]

En cuarto lugar, redes sociales suponen que se implique a personas que no son usuarias de las mismas. Es, por ejemplo, el caso del usuario que sube fotos o publica datos de otros amigos o de personas ajenas a la red social. Entre los derechos que pueden quedar afectados se incluyen el derecho al honor, a la intimidad personal y familiar y a la propia imagen. También provocan conflictos entre el derecho a la libertad de información y expresión y el derecho a la privacidad.

Finalmente, destacar que al darse de baja del servicio no se eliminan permanentemente todos nuestros datos, especialmente los que están en cuentas de otros usuarios. La propia red social cuando tratemos de darnos de baja intentará convencernos de que no es una buena idea y nos preguntará en repetidas ocasiones si estamos seguros de querer hacerlo, apelando a los sentimientos del usuario con frases como "tus contactos y tú no podréis relacionaros", "vas a perderte información esencial de tus amigos", etc. Además nos pedirá que le digamos al programa la causa del cese en la plataforma y que rellenemos un cuestionario. Seguidamente, nos indicará que nuestra cuenta quedará en suspensión durante un tiempo (generalmente de uno a tres meses) permitiéndonos reactivarla en cualquier momento con solo introducir de nuevo nuestro

[12] Exigencia que recoge el art. 13 del Real Decreto 1720/2007, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, relativo al consentimiento para el tratamiento de datos de menores de edad.

nombre de usuario y contraseña. Finalmente, aunque nos demos de baja, todo lo que hayamos publicado en la red, fotografías y videos, perdurarán en la misma, sin posibilidad de borrarlos si hemos "etiquetado a más contactos" o compartido la información con estos, que es lo frecuente en estas plataformas.

4. NORMATIVA Y ÁMBITO DE APLICACIÓN

Identificados los problemas y desafíos jurídicos que presentan las redes sociales para el futuro de su régimen jurídico, abordamos ahora un apartado dedicado al análisis de la normativa actual que regula este medio de comunicación. Para facilitar su comprensión, se ha dividido la normativa en cinco apartados claramente definidos:

4.1. Servicios de la Sociedad de la Información

-Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y Comercio Electrónico (LSSICE)-

En el año 2002, cuando se aprobó esta Ley, los sitios web de mensajería instantánea como *Messenger* estaban muy de moda, pero las redes sociales aún no existían, lo que supone que las leyes actuales requieren adaptarse a las nuevas tecnologías de las información (TIC). La LSSICE se encarga de regular las obligaciones de los prestadores de servicios electrónicos en las redes de telecomunicaciones (art. 1). En cuanto al ámbito de aplicación subjetivo, por prestadores de servicios de la sociedad debe entenderse que son aquellos que prestan servicios a distancia, por vía electrónica y a petición individual del destinatario normalmente a título oneroso, es decir, como manifestación de una actividad económica[13].

Por tanto, todo sitio web que reúna los requisitos del artículo 2 deberá cumplir con las obligaciones contenidas en esta normativa, sin perjuicio de lo establecido en tratados o convenios internacionales que sean aplicables. Dichos requisitos son, que el prestador de servicios de la sociedad de la información (responsable del sitio web) se encuentre establecido en España, entendiéndose por establecido en España cuando su residencia o domicilio social se encuentren en territorio español, siempre que éstos

[13] MARTÍNEZ GUTIÉRREZ, R., "Servicio Público Electrónico y Responsabilidad", *Revista Española de Derecho Administrativo*, Número 155, Cizur Menor (Navarra), 2012, p. 313, pp. 291-318.

coincidan con el lugar en que esté efectivamente centralizada la gestión administrativa y la dirección de sus negocios, atendiéndose siempre al lugar en el que se realice dicha gestión o dirección.

Asimismo, en el caso de que el prestador se encuentre en otro Estado, también quedará sometido a la normativa Española si ofrece sus servicios a través de un establecimiento permanente situado en España, considerándose que se opera mediante un establecimiento permanente situado en territorio español cuando se dispone en el mismo, de forma continuada o habitual, de instalaciones o lugares de trabajo, en los que realice toda o parte de su actividad. E incluso, si a pesar de ser propiedad y alojarse en servidores externos a la Unión Europea, dirige sus servicios específicamente al territorio español. Teniendo en cuenta estos criterios, y sobre todo el tercero, todas las redes sociales que podemos usar desde España están sometidas a esta normativa y, por tanto, a las obligaciones que impone.

Estas se concretan en un deber de información general (art. 10) consistente en disponer de los medios que permitan, tanto a los destinatarios del servicio como a los órganos competentes, acceder por medios electrónicos, de forma permanente, fácil, directa y gratuita a información relativa al mismo, como es su nombre o denominación social, profesión que ejerce si la misma está regulada, información fiscal, precio de los productos que ofrece etc.

Y también, un deber de retención de datos de tráfico relativos a las comunicaciones electrónicas (art. 12). Se trata de una obligación que enlaza directamente con el "derecho al olvido" que analizaremos más adelante. En virtud de este precepto, los prestadores de servicios de alojamiento de datos deberán retener sólo aquéllos imprescindibles para identificar el origen de los datos alojados y el momento en que se inició la prestación del servicio. Además, no podrán utilizar los datos retenidos para fines distintos de los indicados en el apartado siguiente u otros que estén permitidos por la Ley, y deberán adoptar medidas de seguridad apropiadas para evitar su pérdida o alteración y el acceso no autorizado a los mismos.

Es preciso tener en cuenta que en el contexto de una red social, en el que su finalidad primordial es el aglutinamiento de datos personales de los usuarios, dar cumplimiento a estas obligaciones es fundamental. Por tanto, ésta no podrá obtener de

nosotros más datos de los necesarios para gestionar nuestro perfil en la red y con respecto a los que cada usuario suministre, deberá asegurar la finalidad para la que se han aportado y medidas de seguridad para evitar su pérdida o alteración.

Por tanto los operadores que explotan redes de comunicaciones electrónicas están llamados a velar de forma prioritaria y especial por la privacidad electrónica[14]. Un eficaz sistema de protección de datos en el ámbito de las comunicaciones electrónicas exige rebasar incluso la solución estrictamente jurídica, para abrazar cualesquiera medidas e iniciativas que coadyuven a encauzar el problema, en una suerte de estrategia común acorde a la magnitud y especiales que presenta. La implicaciones técnicas de las comunicaciones electrónicas, en este caso, de las redes sociales y la dimensión extraterritorial de Internet, representan tales obstáculos para la protección de la vida privada, que impiden renunciar a nuevas vías como la autorregulación y autocontrol de los sectores implicados[15].

-Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información-

Esta Ley pretende eliminar las barreras existentes en la expansión y uso de las tecnologías de la información y de las comunicaciones y garantizar los derechos de los ciudadanos en la nueva sociedad de la información. Con respecto a las redes sociales destacar que se incluye un nuevo artículo 12 bis con la rúbrica "obligaciones de información sobre seguridad". Establece que los proveedores de servicios de intermediación establecidos en España que realicen actividades consistentes en la prestación de servicios de acceso a Internet, estarán obligados a informar a sus clientes de forma permanente, fácil, directa y gratuita, sobre los diferentes medios de carácter técnico que aumenten los niveles de la seguridad de la información y permitan, entre otros, la protección frente a virus informáticos y programas espía, y la restricción de los correos electrónicos no solicitados. Además, deberán informar a sus clientes de forma permanente, fácil, directa y gratuita sobre las medidas de seguridad que apliquen en la provisión de los mencionados servicios.

[14] "Sobre la dimensión subjetiva del derecho a la protección de datos personales en el ámbito de las telecomunicaciones La protección de datos personales en las autopistas de la información", *XII Encuentro sobre Informática y Derecho*, Madrid, 1999, pp. 105-128.

[15] BALLESTEROS MOFA, L.A., *La privacidad electrónica. Internet en el centro de protección*, Valencia, 2005, pp. 307-315.

Este precepto obliga, por tanto, a las redes sociales que nos prestan sus servicios a mantener mayores niveles de seguridad y proporcionar más información a sus usuarios.

4.2. Protección de Datos Personales

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

Como bien observa BARRIUSO[16] con respecto a la información depositada por los usuarios de las redes sociales virtuales, "cuantos más datos estén disponibles para el análisis y más poderosas sean las herramientas de análisis, más significativa será la información que se obtenga y más riesgos habrá de vulnerar la intimidad y las prescripciones sobre protección de datos personales". Esta consecuencia parece inevitable si se piensa que las redes sociales son escenarios en los que se motiva psicológicamente a los usuarios a ampliar informaciones personales que posteriormente permiten un rastreo de perfiles cada vez más completos.

La necesaria regulación de esta cuestión se encuentra en el título II de la Ley de protección de datos[17]. Así, el art. 4 dispone que "los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido". Y añade que "no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos". Pero resulta complejo determinar que datos son los adecuados y pertinentes para figurar en una red social, sobre todo si se tiene en cuenta que una de sus principales finalidades es recoger datos de sus usuarios para compartirlos con otros usuarios y fomentar que se conozcan.

El artículo 5 regula el derecho de información en la recogida de datos. Exige que los interesados sean previa y expresamente informados de la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de

[16] BARRIUSO, C., "Las Redes Sociales y la Protección de Datos Hoy", *Anuario Facultad de Derecho*, número II, Universidad de Alcalá, 2009, p. 304, pp. 301-338.

[17] Esta norma se completa con el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de Desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal; y con la Ley 25/2007 de octubre, de Conservación de Datos relativos a las Comunicaciones Electrónicas y a las Redes Públicas de Comunicaciones.

éstos y de los destinatarios de la información, así como de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición. Cuando los datos de carácter personal no hayan sido recabados del interesado, éste deberá ser informado de forma expresa, precisa e inequívoca, por el responsable del fichero o su representante, dentro de los tres meses siguientes al momento del registro de los datos, salvo que ya hubiera sido informado con anterioridad, del contenido del tratamiento y de la procedencia de los datos. Esto último es lo que sucede cuando un contacto sube fotografías nuestras a la red social, ésta está obligada advertirnos de dicha subida y de que se ha vinculado esa fotografía a nuestros datos o perfil de usuario (lo que comúnmente se conoce como etiquetar a un contacto en una foto).

Por otro lado, el artículo 15 regula el derecho de acceso, que supone que el interesado puede solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos. Más adelante, en el análisis relativo al "derecho al olvido" veremos que las redes sociales no siempre han cumplido con este obligación, siendo un estudiante austríaco, Max SCHREMS[18], de 24 años, el primero en obtener realmente todos los datos que FACEBOOK poseía sobre él.

Finalmente, el artículo 16 contiene el derecho de rectificación y cancelación, que se concreta en la obligación para el responsable del tratamiento de los datos de hacer efectivos estos derechos del interesado en el plazo de diez días. Tampoco se da cumplimiento a este mandato ya que una vez nos damos de baja en la red social nuestros datos permanecen en la misma, y la cuenta de la que somos usuarios no queda deshabilitada hasta pasar un plazo superior, normalmente un mes, teniendo siempre el usuario la opción de recuperarla con sólo introducir su nombre y contraseña de nuevo en el servidor. De forma que, por regla general, la red social mantiene los datos por si los usuarios quieren volver en un futuro.

4.3. Protección de la Privacidad, Honor, Intimidad y Propia Imagen

-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-

[18] SCHREMS, M. (1987, Salzburgo) estudió en la Facultad de Derecho de la Universidad de Salzburgo. En 2011 interpuso demanda contra FACEBOOK ante la sede europea de la compañía en Irlanda, denunciando el excesivo volumen de datos que esta red social poseía sobre él.

Cabe preguntarnos, al amparo de esta ley, si es posible que por el uso de una red social se llegase a ocasionar una intromisión ilegítima en el honor, intimidad o imagen de una persona. Sobre todo teniendo en cuenta que esta protección del derecho al honor y la intimidad personal y familiar y el pleno ejercicio de los derechos ciudadanos frente al uso de las modernas técnicas informáticas se encuentra también recogida expresamente en el artículo 18.4 CE[19]. La respuesta es que, como en cualquier otro medio de comunicación, dicha intromisión es perfectamente plausible.

Para determinar los posibles escenarios acudimos al artículo 7 donde se identifican como intromisiones ilegítimas entre otras: A) La divulgación de 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; B) La revelación de datos privados de una persona o familia conocidos a través de la actividad profesional u oficial de quien los revela; C) 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[20]; D) La utilización del nombre, de la voz o de la imagen de una persona para fines publicitarios, comerciales o de naturaleza análoga y E) La imputación de hechos o la manifestación de juicios de valor a través de acciones o expresiones que de cualquier modo lesionen la dignidad de otra persona, menoscabando su fama o atentando contra su propia estimación.

Por tanto, las redes sociales pueden convertirse en un medio para afectar el honor y la integridad personal de los individuos, cuando ellas se convierten en vehículo para dos tipos de conductas que pueden menoscabar estos bienes jurídicos: la injuria y la calumnia. La injuria es la conducta que lesiona la reputación e imagen de un individuo, imputándole un hecho deshonroso que dañe o menoscabe su patrimonio moral. Por su parte la calumnia, es una acción en la cual se hace una acusación de

[19] Como bien recuerda LUCAS MORILLO DE LA CUEVA, P., *El derecho a la autodeterminación informativa.* Madrid, 1990, pp. 74 y 135-136.

[20] En particular, el derecho a la propia imagen no impedirá: a) Su captación, reproducción o publicación por cualquier medio, cuando se trate de personas que ejerzan un cargo público o una profesión de notoriedad o proyección pública y la imagen se capte durante un acto público o en lugares abiertos al público. b) La utilización de la caricatura de dichas personas, de acuerdo con el uso social. c) La información gráfica sobre un suceso o acaecimiento público cuando la imagen de una persona determinada aparezca como meramente accesoria.

manera tendenciosa, de mala fe o de forma temeraria, atribuyendo a una persona la comisión de un delito a sabiendas que la conducta atribuida es falsa.

A partir de estas definiciones vemos que los tipos penales de injuria y calumnia son delitos de conducta, no de resultado, y en ese sentido el nuevo escenario de las redes sociales virtuales hace posible atentar fácilmente contra el honor y dignidad de los usuarios de las mismas a través de publicaciones realizadas de manera personal o anónima, para difundir contenidos que pueden afectar el honor y dignidad de quien se presenta públicamente haciendo uso de esta tecnología[21].

Podrían cometer estas intromisiones tanto los usuarios de la red social, como los propios responsables y operadores de las mismas. De hecho, el artículo 12 de la LSSICE obliga a los operadores de redes y a los proveedores de acceso a "retener los datos de conexión y tráfico generados por las comunicaciones establecidas durante la prestación de un servicio de la sociedad de la información por un período máximo de doce meses". El apartado 3º de este precepto precisa que los datos se conservarán para su utilización en el marco de una investigación criminal o para la salvaguardia de la seguridad pública y la defensa nacional, poniéndose a disposición de los Jueces o Tribunales o del Ministerio Fiscal que así los requieran[22].

4.4. Protección de Consumidores y Usuarios

- *Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el Texto Refundido de la Ley General para la Defensa de los Consumidores y Usuarios*[23]-

Como mencionábamos al principio de este trabajo, las redes sociales han adquirido una nueva función, la empresarial o comercial. No es nada raro obtener ofertas de bienes y servicios en el uso diario de estas plataformas y, por tanto, resulta de aplicación esta normativa, sobre todo en lo relativo a la oferta y a la contratación a

[21] ARÉVALO MUTIZ, P.L., "Aproximación a problemáticas jurídicas de las redes sociales virtuales" *Revista Virtual Universidad Católica del Norte*, número 37, Colombia, 2012, p. 27, pp. 62-92.

[22] VALERO TORRIJOS, J., "Responsabilidad administrativa sancionadora", *Deberes y responsabilidades de los servicios de acceso y alojamiento. Un análisis multidisciplinar* (Coord. CAVANILLAS MÚGICA, S.), Granada, 2005, pp. 107-110, pp. 87-114.

[23] La regulación de esta cuestión se completa con la Ley 44/2006, de 29 de diciembre, de Mejora de la Protección de los Consumidores y Usuarios.

distancia (título III del Texto Refundido). Como bien recuerda ROIG[24], "las redes sociales también poseen valor económico y por ello cada vez se crean más ingenios que buscan la información personal de sus usuarios", de manera que la salvaguarda de la privacidad individual sucumbe a los intereses económicos.

4.5. Protección de menores e incapaces

-Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor, de modificación parcial del Código Civil y de la Ley de Enjuiciamiento Civil-

Ya hemos advertido los riesgos que puede suponer el uso de las redes sociales para los menores de edad y sobre todo, cuando rondan los 14 años. La ley que ahora nos ocupa, en su artículo 4 regula el Derecho al honor, a la intimidad y a la propia imagen y advierte que "*la difusión de información o la utilización de imágenes o nombres de los menores en los medios de comunicación que puedan implicar una intromisión ilegítima en su intimidad, honra o reputación, o que sea contraria a sus intereses, determinará la intervención del Ministerio Fiscal, que instará de inmediato las medidas cautelares y de protección previstas en la Ley y solicitará las indemnizaciones que correspondan por los perjuicios causados*". Por tanto vemos que se otorga una especial protección a este derecho en el caso de menores y un papel activo al Ministerio Fiscal para su defensa, quien podrá actuar de oficio o a instancia del propio menor o de cualquier persona interesada, física, jurídica o entidad pública.

En segundo lugar, el artículo 5 del mismo texto legal reconoce a los menores el derecho a buscar, recibir y utilizar la información adecuada a su desarrollo. Seguidamente enuncia en el apartado 2 que los padres o tutores y los poderes públicos velarán porque la información que reciban los menores sea veraz, plural y respetuosa con los principios constitucionales. Por tanto, ¿supone este precepto la obligación para los padres o tutores de controlar la información que reciben sus hijos (o tutelados) por medio de las redes sociales? ¿es realmente esto posible? Recordemos que cualquier menor mayor de 14 años puede darse de alta en las redes sociales (aunque hay usuarios más jóvenes como ya hemos advertido), y puede hacerlo desde cualquier ordenador (no

[24] ROIG, A., "E- privacidad y redes sociales", *Revista de Internet, Derecho y Política*, núm. 9, 2009, p. 42, pp. 42-52.

es necesario el de casa, sirve el de un amigo o el de una biblioteca pública) e incluso desde su teléfono móvil, sin que los padres tengan conocimiento de ello.

En tercer lugar, el art. 12 dispone que la protección del menor por los poderes públicos se realizará mediante la prevención y reparación de situaciones de riesgo. ¿Podemos considerar el uso por un menor de 14 años de una red social una situación de riesgo? ¿Existen actualmente medidas reales y efectivas que eviten que un menor de esa edad se de alta en dichas redes? Una posible medida podría ser que en los colegios se concienciara a los menores del uso de las redes sociales, de los beneficios y problemas que plantean y los riesgos que se pueden producir, al igual que reciben clases de educación sexual.

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

De forma insuficiente, la legislación de protección de datos requiere la intervención de los padres o tutores legales en la prestación del consentimiento para el tratamiento de datos de los menores de catorce años[25]. Concretamente, este Real Decreto, en su artículo 13, se encarga de regular el consentimiento para el tratamiento de datos de menores de edad y dispone que en el caso de los menores catorce años siempre se requerirá el consentimiento de los padres o tutores. Sin embargo, en el caso de los mayores de catorce años, éstos sí que pueden prestar su consentimiento con relación a sus datos personales, salvo cuando la Ley exija la asistencia de los titulares de la patria potestad o tutela.

En segundo lugar, el mismo precepto advierte que en ningún caso podrán recabarse de menores de edad datos que permitan obtener información sobre los demás miembros del grupo familiar, o sobre las características del mismo, como los datos relativos a la actividad profesional de los progenitores, información económica, datos sociológicos o cualesquiera otros, sin el consentimiento de los titulares de tales datos. Ahora bien, podrán recabarse los datos de identidad y dirección del padre, madre o tutor con la única finalidad de obtener la autorización prevista en el apartado anterior. Por

[25] RIESTRA-ABOGADOS, R*egulación legal del web 2.0. Acciones de marketing y redes sociales.* Madrid, 2009, pp. 12-13, www.riestraabogados.com.

tanto, vemos como un menor de edad pero mayor de 14 años podría darse de alta en una red social por su cuenta, ya que tiene capacidad para prestar su consentimiento, mientras que los menores de dicha edad requerirían el consentimiento de sus padres o tutores.

Sin embargo, esta capacidad de los mayores de 14 años requiere cautelas, y por ello en el apartado 3º del mencionado artículo se exige que la información dirigida a los menores deberá expresarse en un lenguaje que sea fácilmente comprensible por éstos. En respuesta a lo anterior y con el fin de proteger a este colectivo, la AEPD[26] se reunió con los proveedores de redes sociales y fruto de esas reuniones, la red social TUENTI procedió a dar de baja a los usuarios menores de 14 años de edad de su red. Por su parte, FACEBOOK anunció en febrero de 2011 que aumentaría a 14 años la edad mínima para darse de alta en la red social.

En tercer lugar, es el apartado 4º del artículo 13 el que mayores dificultades plantea ya que encarga al responsable del fichero o tratamiento de los datos articular los procedimientos que garanticen que se ha comprobado de modo efectivo la edad del menor y la autenticidad del consentimiento prestado en su caso, por los padres, tutores o representantes legales. El problema surge en relación con los mecanismos de control y verificación de la edad, puesto que exige adjuntar fotocopia del DNI y enviarla mediante correo electrónico. Esto ha provocado que los menores de esa edad falsifiquen su DNI, lo que resulta bastante sencillo empleando un programa de diseño gráfico[27], y puesto que lo que la red social recibe es un escaneo o fotocopia, no puede comprobar la veracidad de la misma, luego sigue existiendo una clara falta de control. Una solución efectiva sería acudir a la acreditación de la edad mediante el DNI electrónico, puesto que ya la gran mayoría de personas dispone del mismo y mediante el periférico correspondiente y el puerto USB se podría verificar la edad de forma efectiva. Además, se debería impedir que los usuarios se intentasen volver a registrar con una edad diferente si previamente han sido rechazados por estar por debajo de la edad mínima permitida.

[26] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS.

[27] El programa Adobe Photoshop permite modificar la fecha de nacimiento de una imagen escaneada de un DNI en tan sólo 5 minutos y de forma sencilla.

5. PRINCIPIOS REGULADORES RECOMENDADOS POR LA COMISIÓN EUROPEA

Pese a los problemas regulativos que hemos expuesto anteriormente, es preciso mencionar que los Sistemas de Redes Sociales no se han autorregulado "a ciegas", sino que existen unos principios[28] ideados por la Comisión Europea y publicados en su sitio web "área de *Sociedad de la información*"[29], los cuales fueron elaborados comienzos del año 2009 con el objeto de mejorar aspectos de la privacidad y protección de menores. En cuanto al rango normativo de estos principios, son una aspiración y por tanto, no son preceptivos o jurídicamente vinculantes, aunque se ofrecen a los proveedores de servicios con una fuerte recomendación para su uso. Por su alto interés se recogen aquí sistematizados y analizados:

Principio 1: Fomentar la conciencia y la educación en los usuarios, padres, maestros y cuidadores sobre como recibir información de manera clara y apropiada acerca de la seguridad y las políticas de uso.

Los proveedores deben ofrecer una orientación clara, específica así como materiales educativos diseñados para dar a los niños y jóvenes las herramientas, conocimientos y habilidades necesarias para navegar con seguridad en sus servicios. Además, los padres juegan un papel crucial para que su hijo navegue con seguridad en Internet, debiendo ser capaz de dialogar sobre estos temas de forma abierta e informada.

Principio 2: Asegurar que los servicios son apropiados para la edad del usuario.

Los proveedores deberán considerar si el servicio puede generar riesgos para niños y jóvenes, tratando de limitar la exposición a contenidos potencialmente inapropiados. Entre las medidas que pueden adoptarse podemos mencionar algunas a título de ejemplo: dejando claro cuando los servicios no son apropiados por razón de la edad; tomando medidas para identificar y eliminar a los usuarios menores de edad de sus servicios; impidiendo que los usuarios se intenten volver a registrar con una edad diferente si previamente han sido rechazados por estar por debajo de la edad mínima

[28] *http://ec.europa.eu/información_society/activities/social_networking/docs/se_principles.pdf>*. No es una traducción literal de los principios.

[29] EUROPEAN COMISSION INFORMATION SOCIETY, sitio web, *http://ec.europa.eu/*

permitida; y también, promoviendo la adopción de controles por los padres para que puedan administrar el uso que hacen sus hijos del servicio.

Principio 3: Capacitar a los usuarios a través de las herramientas que ofrece la tecnología.

Los proveedores deben ayudar a los niños y jóvenes en la gestión de la experiencia en su servicio, en particular con respecto a un uso inapropiado o no deseado del contenido. Las medidas que pueden ayudar a minimizar este riesgo pueden consistir en mecanismos para asegurar que los perfiles privados de los usuarios registrados en la edad de 14 a 18 años no están abiertos para su búsqueda; dando a los usuarios el control sobre quién puede tener acceso a su perfil completo así como poder "rechazar" solicitudes de amistad; así como, dar a los usuarios la opción de permitir sólo a los amigos directos enviar comentarios y contenido a su perfil.

Principio 4: Proporcionar una manera fácil de utilizar los mecanismos para informar de las conductas que violen el contenido de las condiciones del servicio.

Los proveedores deben proporcionar un medio para informar sobre contenidos inapropiados o comportamientos contrarios a los recogidos en las directrices de los "Términos del Servicio y las Políticas de Uso". Estos mecanismos deben ser fácilmente accesibles a los usuarios en todo momento y el procedimiento ha de mostrarse comprensible y apropiado para la edad de los usuarios.

Principio 5: Responder a las notificaciones de contenidos y conductas ilícitas.

Tras la recepción de la notificación de presuntos contenidos o conductas ilícitas, los proveedores deben disponer de procedimientos eficaces para revisarlas con rapidez y eliminar el contenido ofensivo cuando proceda.

Principio 6: Alentar y permitir a los usuarios emplear una configuración segura con respecto a su información personal.

Los proveedores deben proporcionar una amplia gama de opciones de configuración de la privacidad, con información de apoyo que anime a los usuarios a ser cautos con lo que publican. Estas opciones deben ocupar un lugar destacado en la experiencia del usuario y ser accesibles en todo momento.

Principio 7: Evaluar los medios para revisar el contenido ilegal y las conductas prohibidas.

Los proveedores deberían evaluar su servicio para identificar los riesgos potenciales para los niños y jóvenes, con el fin de determinar los procedimientos adecuados para examinar las denuncias de imágenes, videos y texto que pueden contener información ilegal, inapropiada o inaceptable, así como contenidos o conductas prohibidas. Hay varios procedimientos que pueden ser utilizados para promover este objetivo, por medio de herramientas técnicas (por ejemplo, filtros) para identificar el contenido potencialmente prohibido o ilegal. Algunos proveedores emplean moderadores que interactúan en tiempo real con los niños o jóvenes.

En definitiva, estos principios promueven la mejora de la protección de la privacidad, de los datos personales, de la concienciación de los usuarios así como la información sobre seguridad que toda Red Social debe tener. Asimismo, tienen por objeto proporcionar orientación a los proveedores de los servicios de las redes sociales sobre el tratamiento que deben proporcionar a los jóvenes.

6. EL CONSENTIMIENTO EN LAS REDES SOCIALES

Como paso previo al análisis del Derecho al olvido, conviene ver el régimen jurídico del consentimiento, pues se configura como un requisito indispensable para todo tratamiento de datos, ya que de no existir el mismo, se podría difundir información que el titular de la cuenta en la red social no quiere que se conozca[30]. Cuando una persona accede por primera vez a una red social rellena un perfil con multitud de datos, lo que le conferirá el *status* de usuario, para lo cual se va a requerir su consentimiento. Es obvio que este consentimiento que se requiere es el del titular de los datos, aunque en el caso de los menores de edad, como hemos expuesto anteriormente, se requiere también el de los padres o tutores.

En cuanto al marco legal, el requisito del consentimiento se encuentra regulado por la normativa sobre tratamiento de datos personales, que recordemos se encuentra

[30] RALLO LOMBARTE, A. Y MARTÍNEZ MARTÍNEZ, R. (Coord.), *Derecho y Redes Sociales*, Pamplona (Navarra), 2010, pp. 117-142.

recogida en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal (LOPD) y en el Real Decreto 1720/2007, de 21 de Diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999. Esta normativa se aplica con independencia de que los datos se faciliten en una plataforma *on line.* Además, en las redes sociales los datos que se facilitan son "personales", tal y como se deduce del art. 3 a) de la ley, que define el dato personal como «cualquier información concerniente a personas físicas identificadas o identificables».

Asimismo, la LOPD en el mismo precepto dice que el consentimiento del interesado es "toda manifestación de voluntad, libre, inequívoca, específica e informada". De esta definición podemos extraer los requisitos del consentimiento, que ahora analizamos:

A. Libre, es decir, al margen de cualquier presión o coacción fAdemás teniendo en cuenta la normativa civil, debe evitarse todo tipo de violencia, intimidación o error. Cabe destacar aquí, que el usuario normalmente proporciona la información creyendo que se encuentra en un entorno privado, "entre amigos", pero como ya hemos adelantado, normalmente introduciendo el nombre de usuario en *Google* o cualquier otro buscador de red ya aparecen muchos de los datos personales consignados en la red social.
B. Informado. Corresponde a los proveedores de los servicios suministrar la información de forma clara y sencilla, puesto que la mayoría de usuarios son jóvenes menores de edad. El problema es que prácticamente ningún usuario de la red social se detiene a leer las condiciones y menos aún cuando las mismas se encuentran redactadas en un documento PDF de más cien páginas, como ocurre con la mayoría de servicios que se prestan en internet.
C. Específico. El titular de los datos consiente para una finalidad determinada, sin embargo, puesto que la información se comparte con otros usuarios ésta puede ser utilizada para otro fin que no era el previamente especificado.
D. Inequívoco, lo que supone que se preste sin dejar lugar a duda o equivocación. Surgen problemas con el consentimiento tácito, puesto que requiere más cautelas y plantea problemas de prueba. Sería el caso en que otro usuario nos etiqueta en una fotografía sin que tan siquiera lo sepamos, hemos aceptado las condiciones

del servicio, pero quizás no queramos que nuestra cuenta de usuario quede vinculada con esa fotografía.

E. Previo. Se tiene que otorgar siempre antes de pasar a ser miembro activo de la red social.

F. Revocable. Hay que partir de la premisa de que se pierde el control sobre la información que se publica en internet, prueba de ello es que cuando nos damos de baja deberíamos poder borrar todos nuestros datos y fotografías.

7. DERECHO AL OLVIDO

En el apartado anterior estudiábamos que el consentimiento otorgado con respecto a nuestros datos queda limitado a finalidades concretas. Por tanto, ¿qué sucede cuando nos damos de baja en una red social y nuestra información personal sigue presente en la red? Podemos definir el derecho al olvido como la capacidad legal de todo individuo de exigir el borrado sus datos personales que consten en la red social de la que ha sido usuario, una vez se dé de baja en la misma[31]. A partir de esta definición se plantean dos cuestiones ¿Realmente las redes sociales conservan todos nuestros datos y fotografías aún cuando nos hayamos dado de baja? ¿Está reconocido éste derecho por la Leyes actuales?

Por lo que respecta a la primera pregunta, un editor de Ars Technica[32] reveló que las fotos borradas de un perfil de Facebook podían seguir estando almacenadas en los servidores de la red social e incluso, permanecer accesibles con un enlace directo al archivo. Por ello, se puso en contacto con los responsables de la red para obtener una explicación. Según le respondió Frederic WOLENS[33], la razón por la que las fotos eliminadas por los usuarios siguen en los servidores años después es puramente técnica. Al parecer los antiguos sistemas que han estado empleando para almacenar imágenes no han sido efectivos a la hora de suprimir su contenido, aunque éste desapareciera

[31] El concepto del derecho al olvido digital surgió por primera vez después de que un sondeo, realizado en Estados Unidos en 2009, revelara la existencia de materiales comprometedores en la red. Un 45% de los empleadores buscaba en Internet información sobre el pasado de los aspirantes a un trabajo. Una tercera parte de los encuestados reconoció que lo que encontraron en la red influyó en el proceso de selección.

[32] http://arstechnica.com/web/news/2009/07/are-those-photos-really-deleted-from-facebook-think-twice.ars.

[33] Portavoz de FACEBOOK.

instantáneamente de los perfiles. Da la sensación de que el problema no ha sido una prioridad para ellos hasta la fecha, aunque aseguran estar trabajando ya en la migración a un nuevo sistema capaz de eliminar completamente las fotos en un máximo de 45 días.

Por tanto, FACEBOOK no borra por el momento nuestras imágenes de la red, pero ¿dispone de más datos nuestros? Partiremos de la batalla personal de un universitario austríaco que empezó con la pregunta ¿qué sabe FACEBOOK sobre mí? y que terminó obligando a la mayor red social del planeta a mejorar los términos de privacidad de cientos de millones de sus usuarios. Se trata del caso del estudiante de derecho *Max SCHREMS*[34], de 24 años, el cual recibió 1.222 páginas en un CD, con datos personales divididos en 57 categorías, como aficiones, gustos, opiniones religiosas, y un largo etcétera, que lo dejó helado. Entre los datos, acumulados durante sus tres años en la red social, le alarmó que aparecieran informaciones y conversaciones que había borrado, pero que Facebook no eliminó definitivamente, las siguió conservando en sus archivos digitales.

"*Cuando se elimina algo de Facebook, todo lo que sucede es que te lo esconden para que no lo veas*", explicaba *SCHREMS*. "*Cada vez que le escribes a otra persona, en realidad lo haces a tres, Facebook siempre está presente*", advertía. La red social analizó de forma sistemática todos sus datos sin pedirle su consentimiento, incluido su parecer cuando apretaba el botón "me gusta" no sólo en la red social sino en cualquier página digital con ese "plug-in".

SCHREMS sostiene que lo que la empresa ofrece -mediante una descarga- a sus usuarios como su "archivo personal" no es toda la información que atesora sobre ellos, sino la que se ajusta a las leyes locales. Sin embargo, su insistencia a través de numerosos correos hizo que a él si le diesen toda la información. "*Un error que expuso a la empresa*", sostiene. El archivo fue la clave para iniciar un pulso con el gigante de Internet que se prolongó en 22 reclamaciones ante el organismo irlandés para la protección de datos (DPC), que acabó dándole la razón.

La sede internacional de Facebook -que agrupa a todos los usuarios salvo los de EE.UU. y Canadá- se encuentra en Dublín, lo que implica que la compañía debe

[34] http://tecnologia.elpais.com/tecnologia/2011/12/25.html.

cumplir con las leyes europeas de protección de datos, que son más estrictas que las estadounidenses. Después de una investigación de tres meses por parte de las autoridades irlandesas, la red social se comprometió a mejorar la privacidad de aproximadamente 500 millones de usuarios que dependen de las oficinas de la empresa en Dublín.

En consecuencia, vemos como nuestros datos actualmente permanecen en el servidor de la red social aunque ya no seamos usuarios de la misma y ello nos conduce a la segunda cuestión, ¿hay alguna ley que obligue a las redes sociales a eliminar nuestros datos y fotografías de internet cuando ya no las utilicemos?

Actualmente, la respuesta es negativa, sin embargo la Unión Europea ha puesto sobre la mesa un plan para proteger a los ciudadanos mediante la reforma de la protección de datos en Europa, que se está debatiendo en el seno de la Comisión Europea (CE) desde el 25 de enero de 2012 y que ha recibido más 3.000 enmiendas. Esta normativa incorporará más obligaciones a las empresas en el modo de gestionar la información y reforzará el derecho a la privacidad de los usuarios para generar más confianza y competitividad.

Por tanto, la propuesta de reglamento[35] que ha diseñado la comisaria de Justicia, *Viviane REDING*, incluirá la obligatoriedad para los países miembros de incorporar en sus legislaciones sanciones "eficaces, proporcionadas y disuasorias" para todas aquellas empresas que operen dentro de la UE y vulneren el derecho de los ciudadanos. Según la exposición de motivos de la propuesta, esta normativa encuentra su justificación en la rápida evolución tecnológica y los nuevos retos que supone para la protección de los datos personales, así como por el enorme incremento del intercambio y la recogida de datos. Dicha tecnología permite que tanto las empresas privadas como las autoridades públicas utilicen datos personales en una escala sin precedentes a la hora de desarrollar sus actividades y también los propios usuarios de internet difunden un volumen cada vez mayor de información personal a escala mundial.

[35] Propuesta de Reglamento del Parlamento Europeo y del Consejo 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 (Reglamento general de protección de datos). Bruselas, 25.1.2012 COM(2012) 11 final; 2012/0011 (COD).

Por tanto, se trata de una revisión que tiene como fin garantizar los niveles de seguridad, de privacidad, de profesionalización y transparencia en el tratamiento de datos. Entre las novedades más destacadas que encontramos, cabe resaltar, la creación de la figura del Delegado de Protección de Datos; nuevas exigencias formales de documentación para los que tratan datos ajenos; el principio de rendición de cuentas; el derecho a la portabilidad (el usuario podrá obtener una copia de los datos alojados en una red social y la libertad de trasladarlos a otra); nuevos cambios en la definición de consentimiento; endurecimiento del régimen sancionador, incluyendo la multa y la advertencia escrita, y finalmente, como novedad más importante, el derecho al olvido, que nos permitirá solicitar un borrado total de nuestros datos en cualquier red social.

Este derecho viene recogido en el artículo 17 del futuro Reglamento y es muy novedoso, pues como hemos visto en la Ley 15/99 sobre protección de datos de carácter personal no aparece recogido como un derecho autónomo, sino que tan sólo recoge los denominados derechos ARCO, es decir Acceso, Rectificación, Cancelación y Oposición. Con la nueva normativa se introduce la posibilidad de ejercitar un derecho de cancelación de datos personales y se subsana la problemática que, por ejemplo, existe entorno a los buscadores de internet. Es decir, para no aparecer en un buscador primero debemos forzar a que los sitios webs que contiene nuestra información la eliminen, de forma que los buscadores dejen de indexarla y no salgamos en los resultados que los ciudadanos obtienen en sus búsquedas. Por tanto, mediante su ejercicio se obliga a que cualquier sitio web o red social que almacene datos estará obligado a suprimirlos de inmediato y abstenerse de darles más difusión si el titular de los mismos lo solicita[36].

En cuanto al ejercicio de este derecho, se puede hacer valer cuando concurran algunos de los siguientes supuestos:

A. Cuando retiremos el consentimiento para su tratamiento o haya expirado el plazo de conservación
B. Cuando los datos ya no son necesarios en relación con los fines para los que fueron recogidos.

[36] IVARS, J., *Propuesta reglamento europeo de protección de datos, especial atención al derecho al olvido*, 2013. Disponible en: http://www.elderecho.com/www-elderecho-com/Propuesta-reglamento-proteccion-datos-especial-atencion-olvido_11_574930001.html.

C. Cuando exista oposición del interesado para el tratamiento de datos.

D. Cuando el tratamiento no se ajusta a la normativa.

Asimismo, cabe la posibilidad que durante el transcurso del tratamiento de los datos la empresa, sitio web, red social o en definitiva el responsable del tratamiento hubiera hecho públicos los datos, en ese caso estará en la obligación de adoptar las medidas necesarias, ya no solo organizativas, sino que también técnicas, con el fin de informar a los terceros sobre la solicitud que el interesado ha realizado para que supriman sus datos.

En resumen, la nueva legislación obligaría a las redes sociales a borrar los datos de una persona de forma inmediata y completa si ésta lo reclama de forma explícita y no existe ninguna razón legítima para retenerlos. Estas compañías deberán minimizar el volumen de datos de sus clientes que recogen y procesan y estarían obligadas a notificar, en un plazo de 24 horas, tanto a los interesados como a las autoridades nacionales de protección de datos de cualquier violación de la seguridad. Por tanto, la nueva legislación supondrá un conjunto único de reglas sobre protección de datos, válido de forma inmediata, una vez aprobada por los Gobiernos y la Eurocámara, en toda la UE.

8. ANÁLISIS DE UNA RED SOCIAL: FACEBOOK

Para la elaboración del presente artículo acogemos la premisa de que la mejor manera de conocer la realidad de un sistema y los problemas que plantea es formar parte del mismo. Por ello, me he dado de alta como usuario en la red social *Facebook*, dada su popularidad y el gran número de seguidores que tiene.

En la página de inicio de ésta red social, si procedemos al registro advertiremos una primera cuestión, el control de la edad[37]. Facebook requiere que todos los usuarios proporcionen su fecha de nacimiento verdadera para comprobar su autenticidad y permitir el acceso solamente al contenido apropiado a la edad del usuario, el cual luego

[37] El art.13 del RD 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, exige el consentimiento de los padres o tutores para poder procederse al tratamiento de datos personales de menores de 14 años.

puede ocultar esta información (cuyo uso se rige por la Política de privacidad de Facebook) en su perfil. Como ya adelantábamos antes, con introducir una fecha de nacimiento que nos acredite una edad superior a los 14 años no tendremos ningún tipo de problema para obtener nuestra cuenta.

En segundo lugar, tras introducir los datos de nombre, apellidos, correo electrónico y contraseña, se nos solicitará que agreguemos contactos. Si le damos a "saltar este paso" nos aparecerá este mensaje: "Las personas que llevan a cabo este paso, por lo general encuentran hasta 20 amigos, y Facebook es mucho más divertido con amigos. ¿Seguro que quieres omitir este paso?".

En cuanto al proceso para añadir amigos a nuestra cuenta, se efectúa mediante una solicitud de amistad que el usuario receptor tendrá que confirmar. Como medida disuasoria Facebook nos pedirá que enviemos la solicitud en cuestión únicamente si le conocemos personalmente. Además, una vez agregado un contacto a nuestra cuenta el servidor nos muestra constantemente y de forma aleatoria los amigos de nuestro contacto para que, si los conocemos, les enviemos una "petición de amigo" y extender el alcance de la red social. Hay que decir que es un mecanismo que funciona muy bien puesto que nada mas agregar un contacto si tenemos amigos o conocidos en común enseguida nos llegaran sus peticiones de amistad para que les agreguemos como contactos, ya que el servidor les habrá comunicado que ahora su contacto tiene un nuevo amigo, es decir, nosotros.

En tercer lugar, FACEBOOK pasa a requerirnos información sobre nuestro perfil, la cual se concreta en que designemos nuestro instituto, universidad y empresa. Finalmente, el programa nos pedirá una fotografía que podremos hacer con la web cam del dispositivo con el cual hayamos accedido a la red social o seleccionar una de nuestra galería de imágenes. Primera fotografía nuestra en internet sobre la cual ya no vamos a tener el "control absoluto".

En cuarto lugar, podemos plantearnos si existe alguna medida de seguridad para evitar que otra persona cree una cuenta de forma fraudulenta con nuestros datos. Cuando nos registramos en una red social por lo general ésta solicita un correo electrónico válido a partir del cual generar una cuenta de usuario. Si otra persona emplea nuestro correo electrónico a estos efectos, el servidor envía a dicho correo una

notificación para que confirmemos que realmente somos el propietario del mismo y evitar fraudes. Dicha confirmación pasa por ofrecernos un código que deberemos introducir en la ventana que presenta la red al efecto. Esta medida evita que se den de alta en la red social con una cuenta de correo electrónico de la que seamos titulares pero no evita que alguien pueda crear una cuenta con nuestros datos empleando un correo suyo.

En quinto lugar, por lo que respecta a la política de privacidad, hay que acudir al menú de política de uso de datos, donde hay información sobre los datos que *Facebook* recibe de sus usuarios. Además de la información personal que facilitamos en el registro y la que nuestros contactos pueden introducir sobre nosotros cuando, por ejemplo, nos etiquetan en una fotografía, esta red social también recaba información cuando el usuario mira el perfil de otra persona, envía un mensaje a alguien, busca una página o a un amigo, o hace clic en un anuncio. Asimismo, cuando el usuario publica fotos o vídeos *Facebook* puede recibir información adicional (o metadatos) como la hora, la fecha y el lugar en el que se tomó la foto o el vídeo. E incluso, recoge también datos del ordenador, teléfono móvil u otro dispositivo que el usuario emplee para acceder al servidor lo que puede incluir la dirección IP, la localización, el tipo de navegador que ha usado o las páginas que ha visitado.

Por tanto, *Facebook* sabe mucho de nosotros (realmente demasiado) pero al menos nos permite configurar nuestra privacidad frente a terceros. De esta forma, en nuestra cuenta de usuario podemos elegir quien tiene acceso a nuestro perfil, si sólo amigos o toda la red social y que información personal nuestra será accesible para los demás. Ahora bien, deberá ser el usuario el que configure estos extremos ya que por defecto las opciones de privacidad serán las menos restrictivas lo que supone que alguien que no conozca los riesgos o no sea muy ducho con la informática quizás comparta más información de la que le gustaría o de la conveniente si, por ejemplo, se trata de un menor.

En sexto lugar, el sistema de notificaciones es simplemente magnífico, *Facebook* nos avisará de todo lo que les suceda a nuestros contactos, y no solo cuando estemos usando su interfaz sino que puede enviarnos correos electrónicos e incluso mensajes a nuestro móvil con las últimas novedades de la red social y de sus miembros.

Por supuesto estas notificaciones se pueden desactivar aunque el proceso de configuración, al igual que sucede con el de privacidad, no es muy sencillo y accesible.

En séptimo lugar, una de las acciones más comunes que realizan los usuarios es subir o descargar fotografías. Es el elemento más diferenciador de las redes sociales con los *chats* y por supuesto uno de los que más problemas puede generar como ya hemos visto. El proceso de subida y descarga de imágenes es muy sencillo, basta con seleccionar en la interfaz las que deseemos subir (deberán estar previamente almacenadas en el disco duro de nuestro ordenador, teléfono o memoria flash) y *Facebook* se encarga del resto. Igualmente de sencillo es descararlas y aunque es una opción que se puede bloquear por el usuario con una simple captura de pantalla tendremos la imagen que queramos a nuestra disposición[38].

Finalmente, haremos una referencia al muro. Se trata de un espacio virtual en nuestro perfil en el cual podremos escribir cualquier opinión, inquietud o reflexión con el objetivo de compartirla con nuestros amigos o bien con toda la red social, lo cual dependerá de la configuración que adoptemos en las preferencias del mismo. Es una herramienta muy útil para generar debates con nuestro contactos o proponerles actividades, pudiendo estos hacer clic en un plug-in denominado “me gusta” con el que nos advierten que nuestra publicación es de su agrado. Con esto hemos visto todas las posibilidades que una red social ofrece, pero también todas las dificultades y riesgos que presentan, destacando especialmente la complejidad de algunos menús (consultar y configurar nuestra privacidad, desactivar notificaciones) mientras que otras tareas como agregar amigos o subir fotografías son muy sencillas y efectivas.

9. CONCLUSIONES

Las redes sociales llegan para quedarse, son una magnífica forma de intercomunicarse con nuestros conocidos y amigos desde cualquier lugar y en cualquier momento y no solo eso, sino que también nos permiten intercambiar todo tipo de

[38] Para realizar una captura de pantalla en el sistema operativo Windows, basta con pulsar la tecla "IMPR" y luego pegar la imagen en algún programa de edición como "PAINT". De esta forma todo lo que mostraba el monitor de nuestro ordenador queda plasmado en la nueva imagen que hemos creado (incluida la imagen que estaba bloqueada para su descarga por el usuario de la red social), pudiendo guardarla posteriormente en el popular formato "JPG".

información e imágenes de una forma cómoda, sencilla y rápida. Sin embargo, el hecho de aglutinar tanta información en la red, el tratamiento que ésta recibe o puede llegar a recibir, las configuraciones por defecto de estas plataformas sociales y el uso masivo que hacen de ellas los menores suponen un nuevo desafío para el Derecho.

Se trata de situaciones que generan riesgos que las leyes actuales o no prevén, o los regulan de forma deficiente. Ya hemos visto como desde la Unión Europea se está avanzando en la cuestión con principios reguladores y una propuesta de Reglamento que reconozca el derecho al olvido, pero aún queda un largo camino por recorrer. Sabemos que el Derecho por regla general sigue la pauta "acción-reacción", es decir, surge un problema e introduce soluciones, pero en el caso de las redes sociales vemos como las soluciones no llegan y las que se aportan son ineficaces (como el límite de edad para darse de alta, que no se está respetando). Mientras tanto, este fenómeno social sigue creciendo a pasos agigantados y cada día aumenta el número de usuarios que se exponen al riesgo, siendo la mayoría jóvenes que reciben el mismo tratamiento que un usuario mayor de edad.

Facebook, Tuenti, Twitter, Google+, Hi5, Bebbo, Linkedin, Myspace, Xing y muchas otras, son las herramientas de comunicación de ahora y del futuro y en consecuencia han creado nuevas necesidades para la sociedad actual como son la posibilidad de informar a familiares, amigos y conocidos de los sucesos y opiniones del día a día; compartir con ellos las fotografías del último fin de semana en pocos minutos y recibir notificaciones de lo que hacen las mayores comunidades sociales del mundo. Pero la mayor necesidad de todas es que los usuarios puedan disfrutar de estos servicios de forma segura, consciente e informada y para ello la regulación jurídica debe seguir avanzando.

10. BIBLIOGRAFÍA

ARÉVALO MUTIZ, P.L., "Aproximación a problemáticas jurídicas de las redes sociales virtuales" *Revista Virtual Universidad Católica del Norte*, número 37, Colombia, 2012.

BALLESTEROS MOFFA, L.A., *La privacidad electrónica. Internet en el centro de protección*, Valencia, 2005.

BARRIUSO, C., "Las Redes Sociales y la Protección de Datos Hoy". *Anuario Facultad de Derecho*, número II, Universidad de Alcalá, 2009.

CORRIPIO GIL DELGADO, Mª.R. Y FERNÁNDEZ ALLER, C., "La protección de datos personales en las autopistas de la información", *XII Encuentro sobre Informática y Derecho*, Madrid, 1999, pp. 105-128.

EUROPEAN COMISSION INFORMATION SOCIETY, sitio web, *Http://ec.europa.eu/*

IVARS, J., *Propuesta reglamento europeo de protección de datos, especial atención al derecho al olvido*, 2013. Disponible en: http://www.elderecho.com/www-elderecho-com/Propuesta-reglamento-proteccion-datos-especial-atencion olvido_11_574930001.html.

LUCAS MORILLO DE LA CUEVA, P., *El derecho a la autodeterminación informativa.* Madrid, 1990.

MARTÍNEZ GUTIÉRREZ, R., "Servicio Público Electrónico y Responsabilidad", *Revista Española de Derecho Administrativo*, Número 155, Cizur Menor (Navarra), 2012.

OBSERVATORIO DE LA SEGURIDAD DE LA INFORMACIÓN, *Redes Sociales, Menores de Edad y privacidad en la Red*, INTECO (Instituto Nacional de Tecnologías de la comunicación), 2007, www.inteco.es.

RALLO LOMBARTE, A. Y MARTÍNEZ MARTÍNEZ, R. (Coord.), *Derecho y Redes Sociales*, Pamplona (Navarra), 2010.

RIESTRA-ABOGADOS, R*egulación legal del web 2.0. Acciones de marketing y redes sociales.* MADRID, 2009. www.riestraabogados.com

ROIG, A., "E- privacidad y redes sociales", *Revista de Internet, Derecho y Política*, número 9, 2009.

VALERO TORRIJOS, J., "Responsabilidad administrativa sancionadora", *Deberes y responsabilidades de los servicios de acceso y alojamiento. Un análisis multidisciplinar*, (Coord. CAVANILLAS MÚGICA, S.), Granada, 2005.