LA TUTELA DE LA INFORMACIÓN PERSONAL Y EL USO DE LAS REDES SOCIALES

The protection of personal data and the use of social networks

Trinidad Vázquez Ruano*

RESUMEN: El uso que en la actualidad se está haciendo de las redes sociales por parte de los usuarios y entidades de la Red reporta numerosas ventajas. Pues se trata de canales que permiten distribuir información de forma fácil y sin apenas limitaciones. Lo que propicia mayores márgenes de comunicación. Sin embargo, ello no obsta a que se planteen determinados aspectos en sentido negativo. En particular, en cuanto al riesgo o amenaza que el uso de este nuevo canal de comunicación implica para la intimidad y, en especial, para la tutela de los datos de carácter personal. Los cuales, como es sabido, tienen en el entorno electrónico una notable importancia, pues en Internet el usuario es activo lo que significa que es él el que ha de acceder y visitar los *sites* que le resulten de interés. Por ello, las entidades establecidas en el nuevo mercado *on line* van a tratar de adquirir cualquier tipo de información sobre los mismos que van a utilizar para captar su atención y atraerlos hacia sus espacios electrónicos. Lo que, en ocasiones, se va a contraponer con la tutela que el ordenamiento confiere a los datos de carácter personal.

ABSTRACT: *The use of social networks currently offers many advantages. The networks are channels that allow you to distribute information in a easy way and without limitations. In addition the networks allow you to send all kinds of information and data. However, difficulties arise certain drawbacks, such as the risk or threat to privacy and, in particular, for the protection of personal data. Personal data are in the electronic environment a remarkable importance. The companies established in the new on-line market are going to try to acquire any type of information and data from the users that will be used to capture your attention and attract them to their electronic sites. Because the subject on the Internet is active. Although the use of certain technical tools for the collection of personal information be contrasted with the protection that the legal system provides for personal data.*

PALABRAS CLAVE: Protección de datos, intimidad, redes sociales, seguridad, derechos.

KEY WORDS: *Data protection, privacy, social networks, security, rights.*

Fecha de recepción: 27-09-2011
Fecha de aceptación: 10-01-2012

I. La seguridad de las comunicaciones en el ámbito electrónico

La información y los datos que se refieren a las personas en particular adquieren en el entono electrónico una importancia específica y ello porque las entidades no sólo van a poder establecerse y desarrollar su actividad en el mercado virtual, sino también ofrecer servicios de manera personalizada y, en su caso,

* Profesora Contratada Doctora. Área de Derecho Mercantil. Universidad de Jaén.

individualizada a los usuarios[1]. La Sociedad de la Información ha permitido el desarrollo de servicios que han surgido del avance de los nuevos medios que se han implementado y de las redes de comunicación electrónicas a través de los que es posible que los usuarios se comuniquen sin apenas limitaciones y, además, obtengan información. Lo que requiere que se garantice la correcta remisión de las comunicaciones electrónicas.

En este sentido, entendemos que la seguridad de las comunicaciones en el ámbito electrónico va a proyectarse en tres ámbitos que están interrelacionados entre si. De un lado, los servicios de autentificación de los datos en relación con la firma electrónica; de otro, el deber que compete a las entidades públicas de garantizar técnicamente el uso y disposición de las redes electrónicas que habilitan; y, por último, la protección de los datos personales y de la intimidad de los usuarios, materia que es la que nos ocupa en el presente trabajo y en la que nos centraremos seguidamente.

En cuanto al primer aspecto, es de destacar la iniciativa de la Comisión Europea sobre *«El fomento de la seguridad y la confianza en la comunicación electrónica: hacia un marco europeo para la firma digital y el cifrado»*[2] en la que ya se puso de manifiesto la necesidad de aumentar la confianza en el uso de las Nuevas Tecnologías por parte de los sujetos que participan en el Comercio Electrónico y de proteger la seguridad de las comunicaciones en el mismo. A fin de cumplir estas exigencias se aprobó un texto normativo de ámbito comunitario sobre Firma Electrónica[3] en el que se plasman los principios que garantizan la seguridad de las comunicaciones en beneficio de los empresarios y de los consumidores y usuarios[4]. Estableciendo, a su vez, la tutela de la libre circulación de bienes y servicios en el mercado interior[5].

---

[1] Vid., DAVARA RODRÍGUEZ, Miguel Ángel, *La protección de los intereses del consumidor ante los nuevos sistemas de comercio electrónico, Estudios y Documentación*, núm. 8, Madrid, 2000, págs. 180-185; FREIXAS GUTIÉRREZ, Gabriel, *La protección de los datos de carácter personal en el derecho español*, Barcelona, 2001, págs. 21-22; VÁZQUEZ RUANO, Trinidad, *La protección de los destinatarios de las comunicaciones comerciales electrónicas*, Madrid, 2008, págs. 130-139 y 149-165; VELÁZQUEZ BAUTISTA, Rafael, *Derecho de las Tecnologías de la Información y las Comunicaciones (T.I.C)*, Madrid, 2001, pág. 89.

[2] Iniciativa de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social y al Comité de las regiones, *'El fomento de la seguridad y la confianza en la comunicación electrónica: hacia un marco europeo para la firma digital y el cifrado'*, de 8 de octubre 1997 (COM (97) 503 y BUE 10-1.997, punto 1.2.157).

[3] En concreto, la Directiva 1999/93/CE, de 13 de diciembre, por la que se establece un marco comunitario para la Firma Electrónica (DOCE L 13/12, 19 de enero de 2000).

[4] El Cdo. 14 de la Directiva 1999/93/CE establece la necesidad de que se equilibren las necesidades de los consumidores y usuarios y las de las empresas.

[5] Art. 4 de la Directiva 1999/93/CE.

Junto a la autentificación de los datos en el entorno electrónico, se prevé que las Administraciones Públicas cumplan el compromiso que les compete de garantizar tanto en la técnica como en la gestión, el uso y disposición de las redes electrónicas que ponen al servicio del público. Tal es el caso, por ejemplo, del deber de informar a los usuarios de la posible existencia de un riesgo en la seguridad de las redes de comunicaciones, indicando si va a suponer un coste añadido que no ha de soportar el proveedor del servicio de comunicaciones, en el supuesto de que lo hubiera[6]. De acuerdo con esta obligación, se ha instado a los proveedores de servicios de comunicaciones electrónicas disponibles al público a aprobar previsiones legales, técnicas y reglamentarias concretas al objeto de alcanzar la seguridad de los servicios que ofrecen.

Por último, como se ha indicado, la seguridad de las comunicaciones electrónicas precisa el respeto del derecho a la intimidad y a la normativa en materia de protección de datos[7]. Pues ello va a traer como consecuencia que los usuarios del entorno electrónico incrementen su confianza en el mismo. En este sentido, pese a que no cabe duda que la implantación de las Tecnologías de la Información de las Comunicaciones se está haciendo de forma progresiva, sin embargo, uno de los problemas esenciales de la adecuada aceptación de las mismas es la inseguridad con la que se enfrenta el usuario ante estos nuevos canales de información y de comunicación[8].

De lo expuesto, se extrae la importancia de garantizar la tutela de los datos y de la información de carácter personal de los usuarios en beneficio de la seguridad de las comunicaciones *on line*. En concreto, respecto de los canales telemáticos que permiten difundir mensajes entre sus usuarios y que en la actualidad también son clave para que las entidades que ejercen la actividad de empresa a través de aquéllos se publiciten, como son las redes sociales. En las que la

[6] Los proveedores de servicios de comunicaciones electrónicas disponibles para el público, cuando sea necesario para proteger la seguridad de los servicios que ofertan, colaborarán con el proveedor de la red pública de comunicaciones respecto de la seguridad de la red, art. 4 de la Directiva 2002/58/CE , de 12 de julio, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas, DOUE L 201, de 31 de julio, 2002). La cual ha sido modificada por la Directiva 2009/136/CE, de 25 de noviembre (DOUE L 337, de 18 de diciembre).

[7] Como se desprende del art. 8.1º y 2º de la Directiva 1999/93/CE respecto de los proveedores de servicios de certificación.

[8] En este sentido se ha manifestado el *Grupo de Trabajo sobre protección de las personas en lo que respecta al tratamiento de datos personales*, órgano consultivo independiente de la UE cuyo objetivo es la protección de los datos y la vida privada, en su Documento de Trabajo de 23 de febrero de 1999 (disponible en: www.europa.eu.int/comm/internal_market/ en/dataprot/wpdocs/index.htm).

seguridad de los datos e información que es de titularidad de los sujetos adquiere una nueva dimensión que va más allá de la garantía de la integridad y la seguridad de las comunicaciones remitidas. Pues se incrementan los riesgos para la intimidad y la protección de los datos personales e, incluso, el derecho al honor y a la propia imagen[9].

II. Protección de los datos de carácter personal y el uso de las redes sociales electrónicas

El uso de una red social, aunque no existe un concepto unitario, puede entenderse en general como un canal de comunicación que permite a los usuarios de la misma acceder a una infraestructura que proporciona un prestador de servicios en la Red para compartir información, comentarios y datos con el resto de personas de la misma a las que va seleccionando y con las que interaccionan[10].

En nuestra opinión, y a pesar de la generalización de su uso[11], el principal problema que cabe plantear es el de la tutela de la información personal o los datos que facilitan los usuarios que participan en ellas. Los cuales no se limitan al nombre, fecha de nacimiento, nacionalidad o nivel de estudios, sino que abarcan diversos campos como las aficiones, ideología, fotografías y videos, entre otros muchos y que pueden precisar, según el caso, una tutela específica[12]. Además de hacer posible que se proporcione información actualizada y en tiempo real[13]. Esto es, indicar dónde se encuentra,

[9] Así se ha puesto de manifiesto en el 'Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online', de la Agencia Española de Protección de Datos (AEPD) y el Instituto Nacional de Tecnologías de la Comunicación (INTECO), pág. 8 (para su consulta: www.agpd.es/portalwebAGPD/canaldocumentacion/ publicaciones/common/Estudios/est_inteco_redesso_022009.pdf).

[10] Véase el *Dictamen 5/2009*, de 12 de junio de 2009, del Grupo de Trabajo 29, *relativo a redes sociales en línea*, pág. 4 (disponible en: www.ec.europa.eu/justice/policies/privacy/ docs/wpdocs/ 2009/wp163_es. pdf).

[11] Al respecto puede consultarse el 'Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online', *op.cit.*, págs. 39-41. Distinguiendo entre las redes sociales generales o de ocio y las profesionales (págs. 46-48 y 49-51, respectivamente).

[12] Pues se trata de datos especialmente protegidos siguiendo lo previsto en el art. 7 de la Ley Orgánica de Protección de Datos de carácter personal (LOPD, publicada en el BOE núm. 298, de 14 de diciembre) y los arts. 2 y 8 de la Directiva 95/46/CE, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (DOUE L 281, de 23 de noviembre).

[13] Véase la 'Resolución sobre Protección de la privacidad en los servicios de redes sociales', *30ª Conferencia Internacional de Autoridades de Protección de Datos y privacidad*, Estrasburgo, 15-17 octubre, 2008, págs. 1-2 (disponible en: www.agpd.es/portalwebAGPD/ canaldocumentacion/conferencias/common/pdfs/30_conferencia_internacional/resolucion_redes_sociales.pdf).

cómo y con quién, qué va a hacer y otra infinidad de datos que, en todo caso, son accesibles de manera pública.

La nota esencial de ello es que si bien los primeros son datos que facilita el usuario de modo directo a través de la cumplimentación de un formulario electrónico para poder ser miembro de esa red; los demás, por su parte, son informaciones que pone al servicio de los miembros de su grupo de manera voluntaria, pero se suele desconocer el destino de las mismas.

La relevancia de los datos personales de los usuarios en el ámbito electrónico hace plantearnos dos aspectos jurídicos fundamentales. El primero, los principios legales que hay que respetar en la obtención de datos facilitados por el sujeto y, el segundo, el empleo de herramientas que sirven para recoger información personal en ausencia de su conocimiento, como comprobaremos a continuación.

II.A. Exigencias normativas en materia de protección de datos personales

El avance de la tecnología y la telemática ha hecho plantear la tutela del derecho a la intimidad de lo usuarios con un ámbito más amplio del habitual y que comprende la facultad del sujeto de controlar y proteger sus datos en cuanto a la digitalización de los mismos[14]. Ello ha sido una necesidad que el legislador comunitario ha previsto, en particular en el entorno electrónico.

En principio, y antes de analizar estos presupuestos normativos que determinan la lícita obtención y tratamiento de los datos que pertenecen a los sujetos, es preciso concretar algunas definiciones de interés. La primera aclaración es qué se entiende por *dato de carácter personal*. La norma comunitaria relativa a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y la libre circulación de los mismos expresamente lo define como *cualquier información concerniente a personas físicas*

[14] Es lo que se ha denominado la 'autodeterminación informativa' (VAZQUEZ RUANO, Trinidad, 'Una nueva proyección del derecho a la intimidad. La autodeterminación informativa', *Revista Crítica de Derecho Privado*, núm. 5, 2008, págs. 49-72). También son de interés los trabajos de ALONSO MARTÍNEZ, Carlos, *Protección de datos de carácter personal. El consentimiento en entidades financieras*, Madrid, 2002, págs. 15-16; MORALES PRATS, Fermín, 'Internet: riesgos para la intimidad', en AA. VV. *Cuadernos de Derecho Judicial, Internet y Derecho Penal,* Madrid, 2002, págs. 67-68; MURILLO DE LA CUEVA, Pablo Lucas, 'La protección de los datos personales ante el uso de la informática', *Anuario de Derecho Público y Estudios Políticos*, núm. 2, 1989-1990, pág. 172; PIÑAR MAÑAS, José Luis, 'Consideraciones introductorias sobre el derecho fundamental a la protección de datos de carácter personal', *Boletín del Ilustre Colegio de Abogados de Madrid*, núm. 35, 3ª época, febrero, 2007, págs. 14-24.

identificadas o identificables[15]. Por tanto, va a ser todo dato o información que si bien en un principio no identifica a una determinada persona, existe la posibilidad de que pueda hacerlo a posteriori.

Por su parte, el tratamiento de los datos de carácter personal se concreta en toda actividad que se aplique a los datos mencionados. Tales como: *recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como su bloqueo, supresión o destrucción*[16]*.* De lo cual se extrae, sin lugar a dudas, que la recopilación, organización y publicación o difusión de la información de un titular constituye un tratamiento de datos en los términos de la norma. Siendo el *responsable* del mismo la *persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que sólo o conjuntamente con otros determine los fines y los medios del tratamiento de datos personales*[17]. Si bien, se matiza que en los supuestos en los que los fines y medios del tratamiento vengan previstos por disposiciones normativas o reglamentarias, el responsable o *los criterios específicos para su nombramiento podrán ser fijados por el Derecho nacional o comunitario.* De otro lado, el que trata información de carácter personal por cuenta del que sea responsable tendrá la consideración de *encargado* del tratamiento, pudiendo serlo una persona física o jurídica, autoridad pública, servicio o cualquier otro organismo[18].

Junto a estas definiciones, como se ha indicado, el legislador ha determinado los presupuestos básicos que han de tenerse en cuenta para la tutela de la información de carácter personal[19]. El texto normativo que de forma genérica establece los que han de respetarse

[15] Art. 2 a) de la Directiva 95/46/CE. Resulta de interés, además, el art. 8 de la Carta de Derechos Fundamentales de la UE (Cumbre de Niza, de 7 de diciembre de 2000) y el art. 2. a) del Convenio 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (Estrasburgo, 28 de enero de 1981, ratificado por España el 27 de enero de 1984, publicado en BOE núm. 274, de 15 de noviembre de 1985 y cuya adopción por el Estado español tiene su razón en el *Acuerdo de Schegen* de 14 de junio de 1985). Esta misma definición es la que ha previsto nuestro legislador en el apartado a) del art. 3 de la LOPD y en el art. 5 1º del Real Decreto 1720/2007, por el que se aprueba el Reglamento de desarrollo de la LO 15/1999 de protección de datos de carácter personal (RLOPD, BOE núm. 17, de 19 de enero) en el que se especifica que puede tratarse de información numérica, alfabética, grafica, acústica, entre otros signos.

[16] Art. 2, apartado b) de la Directiva 95/46/CE.

[17] Art. 2, apartado d) de la Directiva 95/46/CE.

[18] Art. 2, apartado e) de la Directiva 95/46/CE.

[19] Si bien, estos derechos pueden limitarse en razón de la seguridad del Estado, la seguridad pública, la defensa, entre otras circunstancias (arts. 2 y 6 de la Directiva 2002/58/CE).

en la recopilación y tratamiento de los datos personales es la Directiva 95/46/CE[20]. Los cuales se concretan en la necesidad de que los interesados tengan conocimiento de la existencia del tratamiento y la identidad del responsable del mismo, a fin de poder manifestar su consentimiento para ello de modo inequívoco[21]. Esto es, se trata de que cuenten con una información precisa y completa respecto a las circunstancias de la obtención, incluida la facultad de acceder al tratamiento, poder rectificar o solicitar la cancelación de la información personal o, en su caso, oponerse al tratamiento de manera gratuita y siempre que medie causa justificada[22]. Asimismo, se reconoce el principio de calidad de los datos, es decir que la información recabada sea adecuada, exacta, pertinente y no excesiva en relación con los objetivos perseguidos. Los cuales han de ser explícitos y legítimos y deben estar determinados en el momento de solicitar los datos.

En igual sentido, se prevé el principio de confidencialidad de la información que implica que las personas que actúen, bajo el mandato del responsable o encargado del tratamiento, sólo podrán tratar los datos a los que se les haya facilitado el acceso y cuando así se les requiera; y el principio de seguridad que se refiere a la necesidad de que los responsables de los mismos adopten las medidas técnicas y organizativas adecuadas y apropiadas en cuanto a las amenazas que surgen en la tutela de la información personal.

Más específico resulta el contenido de la Directiva 2002/58/CE sobre privacidad y comunicaciones electrónicas que incluye las exigencias que han de regir los tratamientos de datos que los nuevos medios habilitados por la telemática permiten llevar a cabo. El cual se divide en las obligaciones de las personas, públicas o privadas, que efectúan tratamientos de datos y en los derechos de los usuarios cuyos datos son objeto de tratamiento[23].

Los presupuestos a los que cabe referirse de modo particular van a ser: el de confidencialidad de las comunicaciones y de los datos de tráfico de las mismas realizadas mediante redes y servicios de comunicación públicos[24]; el principio de seguridad del tratamiento en

[20] La Directiva 2002/58/CE se remite expresamente a los principios contenidos de forma genérica en la Directiva 95/46/CE en las cuestiones relativas a la tutela de los derechos y libertades fundamentales que no estén cubiertos de forma específica por el mencionado texto legislativo y siempre que las comunicaciones electrónicas no sean de carácter público (arts. 1.2° y 15 y los Cdos. 10, 19, 23, entre otros).

[21] Para ampliar esta información, consultar los arts. 6, 7, 16, 17 de la Directiva 95/46/CE.

[22] Art. 14 de la Directiva 95/46/CE.

[23] En concreto, los arts. 4, 5, 6, 9 y 15 de la Directiva 2002/58/CE.

[24] En cuyo caso se prohíbe la escucha, grabación, almacenamiento u otro tipo de intervención de las comunicaciones o sus datos sin el consentimiento del interesado, con la excepción de que esté legalmente previsto y de que se trate del

el marco telemático que han de respetar los prestadores de servicios de comunicaciones electrónicas[25]; y el deber de destrucción o de hacer anónimos los datos relacionados con los abonados y usuarios cuando no sean necesarios a efectos de transmitir la comunicación[26]. Si bien, en caso de su utilización para la posterior prestación de otros servicios, se plantea la necesidad de obtener el consentimiento del interesado a tal fin.

En un tenor similar se ha pronunciado nuestro legislador que ha previsto unos principios generales que otorgan a los sujetos un control sobre los datos que le pertenecen y, a su vez, un conjunto de facultades específicas relativas a los derechos que puede ejercitar[27]. En cuanto a los primeros, se impone como norma general, la necesidad de obtener el consentimiento inequívoco del titular de los datos personales que van a ser objeto de tratamiento o cesión y que será necesario obtener, salvo que legalmente se hubiere previsto lo contrario[28]. Asimismo es necesario respetar el principio de calidad de los datos y el de información al interesado sobre el sujeto que obtiene la información de su titularidad, los datos recabados y la finalidad que justifica su recopilación[29]. En el caso de que se plantee la cesión de la información a un tercero, el interesado ha de manifestar su conformidad y los fines para los que se ceden tienen que estar relacionados de modo directo con las funciones legítimas del cedente y del cesionario[30].

---

almacenamiento técnico preciso para llevar a cabo la comunicación (art. 5 de la Directiva 2002/58/CE).

[25] Art. 4 de la Directiva 2002/58/CE.

[26] Arts. 6 y 9 de la Directiva 2002/58/CE.

[27] Nos referimos al Título II relativo a los *Principios de la protección de datos* (arts. 4 a 12) y al Título III sobre los *Derechos de las personas* (arts. 13 a 19) de la LOPD respectivamente. Estos últimos son derechos de carácter personalísimo, lo que conlleva su ejercicio efectivo sólo por parte de la persona afectada o su representante legal. Este contenido ha sido desarrollado por el RLOPD, de 21 de diciembre. Vid., ARENAS RAMIRO, Mónica, *El derecho fundamental a la protección de datos personales en Europa*, Valencia, 2006, págs. 303-307; FERNANDO MAGARZO, Mª del Rosario, 'La protección de datos personales en el ámbito de la publicidad', *Revista de la Asociación de Autocontrol de la Publicidad*, núm. 77, julio/agosto, 2003, págs. 30-31; FREIXAS GUTIÉRREZ, *op.cit*., págs. 42-46 y 60-62; PIÑAR MAÑAS, *op.cit.*, págs. 24-30; SERRANO PÉREZ, Mª. Mercedes, *El derecho fundamental a la protección de datos. Derecho español y comparado*, Madrid, 2003, págs. 78-80.

[28] Art. 6 de la LOPD y arts. 14 y 15 del RLOPD, pudiendo ser un consentimiento expreso o tácito porque la norma no concreta su forma. Aunque se establecen unas excepciones a la regla general de la necesidad del consentimiento, como por ejemplo: se permite la obtención de información personal de los usuarios en aquellos casos en los que dicho sujeto hubiera mantenido una relación negocial, laboral o administrativa con la entidad en cuestión y dicha información sea precisa para el cumplimiento o mantenimiento de la misma.

[29] Arts. 4-6 de la LOPD y art.8 del RLOPD.

[30] Arts. 11 y 12 de la LOPD y 10 del RLOPD.

Respecto al responsable del tratamiento o, en su caso, al encargado se impone que cumpla con los presupuestos de seguridad exigidos para lo que será preciso que adopte las medidas técnicas y organizativas necesarias que garanticen la seguridad de los datos; e, igualmente, que atienda el deber de secreto profesional en cuanto a la información tratada.

En cuanto al conjunto de derechos específicos reconocidos al titular de la información de carácter personal cabe destacar el derecho de acceso a la información almacenada, el de rectificación o de cancelación de la misma cuando hubieran dejado de ser necesaria o pertinente para la finalidad que justificó su obtención o registro[31]; la oposición al tratamiento siempre que medie causa justificada y sin que ello le reporte coste económico alguno; el derecho de consulta al Registro General de Protección de Datos y la posibilidad de impugnar las valoraciones. Esta última se refiere al reconocimiento a los sujetos de refutar los actos administrativos o las decisiones privadas a las que sean sumidos y que traigan como consecuencia el análisis de sus conductas cuyo objeto sea únicamente el tratamiento de los datos de carácter personal que proporcionen una definición de su personalidad.

En el supuesto de que estas exigencias normativas no se respetasen el afectado puede presentar su reclamación a la Agencia Española de Protección de Datos o a la equivalente en el ámbito autonómico que es la autoridad competente para resolver estas cuestiones[32]. Pudiendo interponerse contra dicha resolución el pertinente recurso contencioso-administrativo ante la jurisdicción que corresponda. Además, en los supuestos en los que no se hubieran respetado las pautas contenidas en la LOPD y ello hubiere ocasionado al titular de los datos personales un daño o lesión en lo que a sus derechos o bienes se refiere, podrán reclamar ante la jurisdicción ordinaria la correspondiente indemnización de esos perjuicios si se trata de ficheros de titularidad privada[33]. En caso contrario, es decir que sean ficheros de titularidad pública, la responsabilidad se regirá según la norma que regula dicho régimen en las Administraciones públicas.

El cumplimiento de los extremos expuestos, trae como consecuencia la garantía de la seguridad de la información personal de los sujetos que acceden al ámbito telemático. Lo que consideramos que va a repercutir en la confianza de los mismos respecto de la utilización de las Nuevas Tecnologías de forma genérica y de actuales canales de comunicación como las redes sociales de manera específica.

[31] Arts. 4. 5, 6.4 y 30.4 de la LOPD y 27-36 del RLOPD.
[32] Arts. 16 y 17 de la LOPD y Título IX del RLOPD.
[33] Consúltense los arts. 18 y 19 de la LOPD.

II.B. La participación en redes sociales electrónicas

La utilización de una red social implica que el interesado ofrezca información de carácter personal y, en ocasiones, también de terceros que puede ser consultada y tratada por una pluralidad de personas que, en algunos casos, resulta complejo determinar. Por tanto, lo que hace el prestador que ofrece una red social es recabar datos e información que voluntariamente los usuarios aceptan facilitar a cambio de poder participar en la misma y remitir comunicaciones al resto de miembros de la red social con los que se interrelaciona. Poniéndose esa información a disposición del público en general.

En materia de protección de datos personales en las redes sociales cabe distinguir dos etapas. La primera o inicial en la que el usuario ha de registrarse en la red social elegida, en cuyo caso es esencial la configuración de la privacidad del perfil por parte del mismo. La segunda o posterior en la que el sujeto que ya forma parte de esa red social participa como miembro de la misma ofreciendo información que le concierne y en la que resulta de interés no sólo el contenido que se pone a disposición del público, sino también que con éste se pueda perjudicar la intimidad de terceros o vulnerar la protección de sus datos personales.

En un primer momento, debe tenerse en cuenta que la obtención de la información o de los datos directamente del sujeto a través de la cumplimentación de un formulario electrónico va a precisar que se incluyan en el mismo los presupuestos normativos previstos en materia de protección de datos y que han sido indicados con anterioridad. Siendo lícita, por tanto, la obtención de los datos personales si al momento de recopilarlos se han cumplido dichas exigencias y el prestador del servicio ha actuado con la diligencia debida, informando de los extremos necesarios al interesado para que pueda otorgar su consentimiento libre, preciso e informado. A este respecto se exige, como norma general, la obtención de la voluntad inequívoca del interesado para recabar datos básicos que le identifican o pueden hacerle identificable[34], lo que va a suponer que el sujeto ha de estar debidamente informado para manifestarla. Distinta consideración cabe hacer respecto de los supuestos en los

[34] Art. 6 de la LOPD. Además, la norma prevé la necesidad de que el responsable *compruebe* la edad del menor y la autenticidad de su consentimiento o el de sus padres o tutores, pues en el caso de que sea un menor el que vaya a facilitar sus datos para acceder a una red social, según el art. 13 del RLOPD, se exige que si tiene menos de catorce años, será necesario en todo caso el consentimiento de padres o tutores. Los que sean menores pero mayores de catorce años podrán dar su consentimiento, salvo que la ley exija que padres o tutores asistan en la prestación del consentimiento. Precisándose que los datos que se recaban al menor no pueden incluir información de los miembros de la familia, salvo identidad y dirección de los padres o tutores para autorizar el consentimiento.

que se proporcionen datos que ostentan la categoría de especialmente protegidos según los términos de la norma. Nos referimos a los que hacen referencia al origen racial, la salud y la vida sexual del interesado en cuyo caso se requiere que éste otorgue su consentimiento de forma expresa[35] y si se trata de datos que revelan su ideología, afiliación sindical, religión y creencias se precisa que la voluntad se ofrezca de forma expresa y por escrito[36].

La obtención del consentimiento inequívoco del interesado implica la necesidad de que el prestador de servicio que ofrece una red social cumpla el deber de información previo a la recopilación de los datos de los usuarios y que hace referencia tanto a su identidad por ser el responsable del tratamiento, como los datos que se van a recoger, la finalidad que lo justifica y cualquier otra información relevante[37]. La LOPD impone expresamente al prestador de servicios que solicite datos personales al interesado el deber de informarle de manera clara y precisa de[38]: la *existencia del fichero o tratamiento de los datos, la finalidad de la recogida de éstos y los destinatarios de la información; la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición; el carácter obligatorio o facultativo de las respuestas a las preguntas requeridas; las consecuencias de la obtención de los datos o de la negativa a suministrarlos; y la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.* Por tanto, cumpliéndose dichos extremos va a considerarse que la manifestación de la voluntad del sujeto resulta inequívoca porque se ha otorgado con la debida información. Si bien no es ésta la única obligación impuesta al prestador responsable de una red social electrónica en

[35] Art. 7. 3 de la LOPD. Pudiendo emitirse mediante un mensaje de voz o texto, una llamada telefónica o la manifestación personal de la voluntad por parte del interesado.

[36] Art. 7. 2 de la LOPD. Pudiendo ofrecerse mediante un formulario electrónico, la remisión de una comunicación debidamente firmada según la Directiva 1999/93/CE, de 13 de diciembre, sobre Firma Electrónica y la Ley 59/2003, de 19 de diciembre, de Firma Electrónica. Vid., ILLESCAS ORTIZ Rafael, 'La firma electrónica y el Real Decreto Ley 14/1999, de 17 de septiembre', *Derecho de los Negocios*, núm. 109, 1999, págs. 5-10; MADRID PARRA, Agustín, 'Seguridad, pago y entrega en el Comercio Electrónico', *Revista de Derecho Mercantil*, núm. 241, julio/septiembre, 2001, págs. 1198-1203 y 1205-1211; MARTÍNEZ NADAL, Apolonia, *Comercio electrónico, firma digital y autoridades de certificación*, 3ª edic., Madrid, 2001 y *Comentarios a la Ley 59/2003 de Firma Electrónica*, Madrid, 2004.

[37] Art. 5 de la LOPD. En el supuesto de que el interesado sea un menor, se exige que dicha información sea *acorde* con la edad a la que va dirigida. Concretando el precepto que se utilice un lenguaje fácil que permita que los menores entiendan para qué están prestando su consentimiento.

[38] El deber de información por parte del prestador del servicio ha de cumplirse tanto si los datos se han recabado directamente del interesado, como si se han obtenido a través de cuestionarios o de cualquier otra forma (apartado 2º del art. 5 de la LOPD).

materia de protección de datos que, como se ha indicado[39], también ha de respetar el principio de proporcionalidad en la obtención de los datos, el de calidad o el principio de seguridad en el tratamiento de la información, entre otros.

El prestador de un servicio de redes sociales puede respetar las exigencias normativas indicadas bien porque las incluya en los propios formularios electrónicos o a través de ciertas disposiciones de la *política de protección* que los espacios electrónicos ofrecen a los usuarios mediante un enlace en sus páginas. Sin embargo, consideramos que en beneficio de los sujetos participantes debiera hacerse una mención concreta a los efectos que pueden tener para el mismo la publicación de determinada información que le concierne y de la posibilidad de que terceras personas puedan consultarla y tratarla. Además, resulta relevante hacer advertencias acerca de la inclusión de datos, imágenes, videos o información que nos es sólo de su titularidad, sino que afectan a terceros que pueden estar al margen de la red social en cuestión[40].

Ahora bien, distinto planteamiento merece hacerse de la información y los datos relativos a una persona que se facilitan en la segunda etapa aludida. Es decir, los que se van incluyendo tras el momento inicial del registro del usuario en la red social. Pues el sujeto va a ofrecer nuevos datos de manera voluntaria y en tiempo real, no siendo consciente en la mayor parte de las ocasiones de las múltiples opciones de las que disponen las redes sociales para tratar esa información personal o cederla a terceros. En estos supuestos, a pesar de que en un momento previo el usuario consintió la difusión de sus datos al incluirlos en su perfil, es posible que se vulneren ciertos principios jurídicos[41]. Por cuanto el titular de dicha información puede conocer y consentir el almacenamiento de la misma o su cesión, pero cabe que ello se haga sin su conocimiento ni

[39] *Supra II. A.- Exigencias normativas en materia de protección de datos personales.*

[40] En la *30ª Conferencia Internacional de Autoridades de Protección de Datos y privacidad*, *op.cit.*, se puso de manifiesto incluso que las configuraciones que se establezcan por defecto respeten en mayor medida la privacidad de los miembros de las redes sociales (págs. 4-5). También en el 'Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online', *op.cit.*, págs. 15-16, se han previsto recomendaciones específicas sobre seguridad, concienciación o formación, entre otras. Asimismo, el *Dictamen 5/2009*, de 12 de junio de 2009, del Grupo de Trabajo 29, *op.cit.,* pág. 9.

[41] En este sentido, también se ha pronuncia la *30ª Conferencia Internacional de Autoridades de Protección de Datos y privacidad* en su 'Resolución sobre Protección de la privacidad en los servicios de redes sociales', *op.cit.*, págs. 3-4. Vid., CAMPUZANO TOMÉ, Herminia, *Vida privada y datos personales*, Madrid, 2000, pág. 81; CASTILLO JIMÉNEZ, Cinta, 'Protección del derecho a la intimidad y uso de las nuevas tecnologías de la información', *Anuario Jurídico sobre la Sociedad de la Información, Derecho y Conocimiento*, vol. I, 2001, págs. 36-38; DAVARA RODRÍGUEZ, *op.cit.,* págs. 185-187.

autorización. Siendo una práctica generalizada que las redes sociales incluyan la posible cesión de los datos a terceros, pero que no se especifique la información que va a ser objeto de la misma.

En este caso, además, se plantea un problema añadido y que ya ha sido referido. Cual es que los datos que se publican en una red social y cuya difusión se facilita a otras personas, en ocasiones, no sólo pertenecen al ámbito privado del sujeto que los proporciona, sino que afectan a terceros. Tales como las imágenes que se publican o los vídeos que se comparten y en los que aparecen personas que no son usuarios de la red social. De acuerdo con los principios normativos referenciados con anterioridad, dicha información podrá difundirse si el tercero afectado lo hubiera autorizado de manera inequívoca, pues en caso contrario esa publicación va a resultar contraria a Derecho[42].

En definitiva, ha de concluirse que el contenido previsto en las *políticas de privacidad* o en los *avisos legales* que incluye el prestador que habilita una red social ha de ser más completo y preciso respeto del cumplimiento de las exigencias normativos en materia de protección de datos personales. Por cuanto el uso de las redes sociales permite acceder y tratar una importante cantidad de datos tanto de los usuarios, como de terceros que puede ocasionar una intromisión en su esfera privada.

III. Los datos de carácter personal en las redes sociales. nuevas vulnerabilidades

La tutela de los datos de carácter personal en el entorno electrónico no siempre resulta efectiva en la práctica. Pues el avance de la Nuevas Tecnologías ha hecho que surjan novedosas técnicas que permiten obtener información personal de los usuarios eludiendo las exigencias normativas previstas para ello. En el caso de la utilización de las redes sociales es cierto que son los usuarios los que de forma voluntaria y directa ofrecen información que les concierne, pero ello no impide que se produzcan intromisiones en su intimidad y que se lleven a cabo prácticas que resultan contrarias a Derecho[43], como comprobaremos a continuación.

[42] La Agencia Española de Protección de Datos así lo ha resuelto en diversos casos, como por ejemplo: Resolución de la Agencia Española de Protección de Datos PS/00117/2008 (BOE núm. 93, de 17 abril), en el que se procede a imponer una sanción a un sujeto que publica en la Red imágenes obtenidas de la vía pública en las que aparecen personas.

[43] Es el caso de la remisión de mensajes comerciales que no se han solicitado de forma masiva o la suplantación de la identidad de los usuarios (vid., el 'Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online', *op.cit.*, págs. 114-117). Un caso reciente sobre la suplantación de la identidad ha sido resuelto por la Agencia Española de Protección

III.A. La instalación de técnicas de obtención de datos personales

El establecimiento de herramientas electrónicas en el equipo informático de los usuarios que permiten recoger datos de los mismos sin que éstos tengan conocimiento de ello y, por tanto, tampoco hubieran manifestado su voluntad para facilitar esa información adquiere una mayor importancia en el ámbito de las redes sociales[44]. Pues ha de tenerse en cuenta que los datos que se van a recoger y tratar para finalidades distintas de las que justificaron su obtención se encuentran en una plataforma electrónica que es de acceso público.

De todos es sabido que cuando un usuario se conecta a la Red a través de un navegador facilita cierta información que puede considerarse de carácter personal, pues aunque algunos de esos datos no identifican directamente a un determinado usuario, pueden llegar a identificarlo si los relacionamos con otros[45]. Estos son: la *Transmission Control Protocol* o *Internet Protocol*[46]; la versión del programa de navegación y del sistema operativo; el lenguaje que utiliza el usuario; la *home page* de referencia y los archivos *cookies* en el supuesto de que se hubieran previsto. Algunos de estos datos puede que tras la conexión electrónica del usuario o, incluso, durante la misma sean analizados por terceros sin que el sujeto tenga conocimiento de ello[47].

El legislador comunitario a través de la Directiva 2002/58/CE se ha ocupado de la regulación de ciertos programas que se introducen

---

de Datos, Resolución R/01716/2011, en el que la actual pareja de la ex pareja del denunciante creó un perfil en una red social en el que insertó un mensaje obsceno con una fotografía del denunciante. La Resolución confirma la reclamación presentada e impone una sanción económica al denunciado. Para su consulta: www.agpd.es/portalwebAGPD/resoluciones/procedimientos_sancionadores/ps_2011/common/pdfs/PS-00137-2011_Resolucion-de-fecha-27-07-2011_Art-ii-culo-6.1-LOPD.PDF

[44] Así se ha recogido en el 'Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online', *op.cit.*, págs. 70-71 y 112-113.

[45] Vid., RIBAS ALEJANDRO, Javier, 'Riesgos legales en Internet. Especial referencia a la protección de datos personales', en AA. VV. (Coords. MATEU DE ROS/ CENDOYA MÉNDEZ DE VIGO), *Derecho de Internet (Contratación electrónica y Firma digital)*, Navarra, 2000, págs. 154-155; VELÁZQUEZ BAUTISTA, *op.cit.*, pág. 121.

[46] La dirección *TCP/ IP* es la señal de identidad del ordenador dentro de la Red. La Agencia de Protección de Datos de Carácter Personal ha considerado que la dirección IP es un dato tutelado por los principios normativos de protección de datos personales en su *Informe 327/03* (disponible en: www.agpd.es/portalweb/canaldocumentacion/informes_juridicos/otras_cuestiones/common/pdfs/2003-0327_Car-aa-cter-de-dato-personal-de-la-direcci-oo-n-IP. pdf).

[47] La expresión *troyanos electrónicos* se refiere al establecimiento de diversas instrucciones en los programas de ordenador de forma oculta. Vid., VELÁZQUEZ BAUTISTA, *op.cit.*, págs. 244-245.

en el equipo informático de los usuarios sin su consentimiento para acceder a determinados datos, archivarlos y hacer un seguimiento de la navegación electrónica del mismo[48]. Los cuales se consideran instrumentos electrónicos de captación de datos personales que vulneran el derecho a la intimidad, la protección de dichos datos y, en su caso, perjudican la libre navegación en el ámbito electrónico. Es el caso, entre otros, de los *spyware*[49]; los *web bug*[50]; los identificadores ocultos[51]; los gusanos o los *sniffers*[52].

Sin embargo, distinto planteamiento se establece respecto de los archivos *cookies*[53], en cuyo caso se ha previsto como regla general su licitud, siempre que se cumplan unos requisitos determinados[54]. Estos son: el deber de informar al titular de los datos

[48] Considerando 25 de la Directiva 2002/58/CE.

[49] Los programas espía o *spyware* permiten el acceso a diversos datos del ordenador del usuario y, por lo general, se instalan a través de los virus informáticos o un troyano.

[50] Un *web bug* es un gráfico *GIP* de 1x1 píxeles que permite obtener cierta información del usuario, como: la dirección *IP* del ordenador, la *URL* de la imagen, fecha y hora en que fue vista la imagen, el tipo y versión de navegador del usuario o el sistema operativo. El problema es que la imagen es invisible y el usuario no tiene conocimiento de que los datos que ha facilitado se han incluido en el *URL* de la imagen y serán conocidos por terceros. Vid., GUERRERO PICÓ Mª. Carmen, *El Impacto de Internet en el Derecho Fundamental a la Protección de Datos de Carácter Personal,* Pamplona, 2006, págs. 476-478.

[51] Los identificadores ocultos también se usan para localizar páginas electrónicas y contenidos en los buscadores. Los identificadores que no se hallan ocultos son instrucciones que se dan al navegador para que visualice la página de Internet como se haya previsto. Para ampliar esta materia, consúltese GUERRERO PICÓ, *op.cit.,* págs. 478-479.

[52] Los gusanos informáticos perjudican tanto a Internet en general como a los sistemas infectados, en particular. Los *sniffers* son programas que interfieren en el disco duro para obtener información de los mensajes enviados mediante el correo electrónico. Sobre esta materia MORÓN LERMA, Esther*, Internet y Derecho Penal: hacking y otras conductas ilícitas en la Red,* 2ª edic., Pamplona, 2002, págs. 31-32.

[53] Los archivos de texto *cookies* (galletas) realizan un control de la audiencia de un determinado espacio electrónico. Al instalarse un *cookie* se introduce una dirección de dominio que cuando el usuario visita un determinado espacio en la Red el navegador comunicará a los servidores que coincidan con el dominio la existencia del *cookie.* Sobre esta materia: DAVARA RODRIGUEZ, *op.cit.,* págs.181-182 y RIBAS ALEJANDRO, *op.cit*., págs. 155-156 y en *Aspectos Jurídicos del Comercio Electrónico en Internet,* 2ª edic., Navarra, 2003, págs. 66-67.

[54] Cdo. 24 Directiva 2002/58/CE. La Agencia de Protección de Datos (2002), *op.cit.,* págs. 126-129 en la Recomendación Segunda señala la necesidad del consentimiento por parte del interesado y en la Tercera Recomendación el deber de información previo a la colocación, debiéndose además prestar atención al principio de finalidad en la obtención de la información. En igual sentido se ha pronunciado el *Grupo de Trabajo sobre protección de datos de las personas en lo que respecta al tratamiento de datos personales*, en la Recomendación 1/99 sobre el tratamiento invisible y automático de datos personales en Internet efectuado por *software y hardware,* el 23 de febrero de 1999 (disponible en: www.europa.eu.int/comm/internal_market/privacy/docs/wpdocs/1999/wp16es.pdf).

de forma precisa e inequívoca de su instalación en el equipo informático y de los extremos que sean de interés, la obtención del consentimiento de los afectados y la necesidad de que su utilización responda a un fin legítimo. Admitiéndose como finalidades acordes a la norma tanto la valoración de la efectividad del diseño y de la promoción establecida en el *sitio web* desde el que se van a insertar, como la acreditación de la identidad de los sujetos partes de una transacción electrónica[55].

Entendemos que el requisito de su instalación de acuerdo a un objetivo justificado va a ser el primer presupuesto que debe tener en cuenta el servidor *web* responsable de la inserción de archivos *cookies* en el ordenador del usuario que visita la página desde la que se remiten y, cumplido éste, ha de informar al interesado según los presupuestos que se han analizado en el apartado anterior[56]. Si bien, hay que exceptuar el supuesto en el que la información almacenada por los archivos *cookies* o por otro tipo de instrumentos electrónicos similares no resulte ilícita por cuanto dichos datos no sean de carácter personal. Es decir, los archivos se instalan en el disco duro de un terminal electrónico, pero no almacenan datos de su titular, sino mera información técnica.

El cumplimiento del deber de información previo a la instalación de estas herramientas electrónicas de obtención de datos personales exige que se atienda lo indicado en la Directiva 95/46/CE[57]. Al igual que respecto a la manifestación de la voluntad sobre la inserción de las mencionadas técnicas de recopilación de información que pertenece a los sujetos. En este sentido, como se ha adelantado, la regla general es que el interesado consienta el tratamiento de los datos que le conciernen manifestando su voluntad de forma libre, específica e informada[58]. Por tanto el establecimiento de archivos *cookies* va a precisar el consentimiento informado e inequívoco del sujeto afectado.

En el ámbito normativo nacional, siempre que pueda afirmarse que la información almacenada en este tipo de técnicas electrónicas es de carácter personal, los prestadores de servicios que las instalen en los terminales informáticos han de atender las exigencias normativas referenciadas con anterioridad[59]. El legislador ha previsto unos derechos que amparan al titular de la información recogida sin

[55] Véase el Cdo 25 de la Directiva 2002/58/CE.
[56] *Supra II. A.- Exigencias normativas en materia de protección de datos personales.*
[57] El deber de información en la obtención y tratamiento de datos de carácter personal (arts. 10 y 11 de la Directiva 95/46/CE).
[58] Arts. 2 h) y 7 de la Directiva 95/46/CE.
[59] *Supra II. A.- Exigencias normativas en materia de protección de datos personales.*

su conocimiento ni consentimiento, por cuanto se entiende que supone una intromisión ilegítima en su esfera privada[60]. Es el caso del ejercicio del derecho de oposición al tratamiento, el de acceso a los datos recabados, el de modificación o, en su caso, la supresión de los mismos. Así como el derecho tanto de presentar la correspondiente reclamación ante la Autoridad nacional competente en materia de protección de datos y, si fuera necesario, de interponer el recurso judicial que corresponda con la pretensión de que el prestador del servicio cese en la utilización de estos instrumentos electrónicos. Pudiendo obtener por parte del responsable del tratamiento la reparación del perjuicio ocasionado por la actuación ilícita.

Ello, no obstante, salvo que el establecimiento de estas técnicas electrónicas responda a la correcta transmisión de una comunicación *on line* o al cumplimiento efectivo de un servicio expresamente solicitado por el destinatario del mismo.

En conclusión, el problema esencial del uso de las técnicas de obtención de información personal que el afectado desconoce es que, por su especificidad, los derechos que su ilícita utilización vulneran no sólo se refieren a la protección de datos o la intimidad. Pues su instalación sin el conocimiento ni el consentimiento del interesado son amenazas para bienes jurídicos como el secreto de las comunicaciones o la confidencialidad de las mismas e, incluso, una intromisión en la libertad del usuario en cuanto a su actuación en la Red.

III.B. Indexación de perfiles sociales por parte de buscadores electrónicos

La utilización del servicio de redes sociales implica que se ofrezca una importante información que pertenece al ámbito personal o, en ocasiones, a terceros. Si bien es cierto, que según la red social en la que se participe las opciones para privatizar esa información difieren, siendo la tendencia generalizada que sólo esté disponible para las personas a las que previamente el usuario hubiera agregado. Mientras que para el resto esos datos serán ocultos. Pese a ello se plantea un problema y es cuando el usuario decide no formar parte de la misma, en cuyo caso resulta complejo eliminar por completo la información facilitada en un ámbito de alcance indeterminado como lo es el electrónico.

[60] Consúltense los arts. 13 a 19 de la LOPD. También es posible recurrir a soluciones técnicas como el uso de los denominados cortafuegos, técnicas de encriptación, el servidor *proxy* u otros programas de *software* gratuito o compartido (MORALES PRATS, *op.cit.*, pág. 74).

En relación con ello, se añade que es habitual que las redes sociales hagan factible a los motores de búsqueda electrónicos la localización de las identificaciones y la indexación de los perfiles de los usuarios[61]. Lo cual puede ser una nueva amenaza para la tutela de la intimidad y de los datos de carácter personal de los miembros. En particular, cuando se decide no seguir utilizando el perfil de la red social en concreto. Pues en estos supuestos se ofrece la opción de deshabilitarlo, pero estará disponible por si el sujeto decide volver a utilizarlo. Ello supone que esos datos pueden ser consultados por parte de terceros. Así, por ejemplo, en el supuesto de que alguien estuviera interesado en conocer la dirección electrónica o la profesión (o cualquier otra información) de una persona va a incluir en un determinado buscador su nombre y entre los resultados generales que le aparecen estará el perfil del mismo en la red social en la que se hubiera registrado y que ha sido indexado.

El conflicto surge en cuanto que el buscador que ha indexado con anterioridad el perfil que se ha desactivado va a seguir mostrando la información en sus resultados, amparándose en que los datos no se han eliminado del *webmaster* que alberga la red social y que, por ende, esa información está aún disponible. El buscador de Internet es un Prestador de Servicios de Intermediación[62] que, a diferencia del simple Prestador de Servicios de la Sociedad de la Información[63], facilita la *prestación o utilización de otros Servicios o el acceso a la información.* Por lo que la norma le reconoce un régimen especial de responsabilidad[64]. En el caso que nos ocupa, el prestador de intermediación que facilita instrumentos de búsqueda electrónicos no será responsable, a menos que tenga conocimiento

[61] Según se indica en el 'Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online', *op.cit.*, págs. 85 y 113-114. En igual sentido, se ha expuesto en la *30ª Conferencia Internacional de Autoridades de Protección de Datos y privacidad, op.cit.,* pág. 2. Esta cuestión ha sido abordada en otras ocasiones en las que se ha enjuiciado la conducta de los buscadores que mantienen información en Red de los usuarios. Tales como, la Resolución de la Agencia Española de Protección de Datos TD/00814/2007, de 7 abril 2008. Para su consulta: www.agpd.es/portalwebAGPD/resoluciones/tutela_derechos/tutela_derechos_2008/.

[62] Apartado b) del Anexo de la LSSIyCE (Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, BOE núm. 166 de 12 julio) que reproduce el contenido del art. 2 de la Directiva 2000/31/CE, de 8 de junio (relativa a determinados aspectos jurídicos del comercio electrónico en el mercado interior, DOUE L 178, de 17 julio). Los cuales van a ser los que ofrecen acceso a Internet; transmisión de datos por redes de telecomunicaciones; copia temporal de páginas de Internet que solicitan los usuarios; alojamiento de los servidores propios y la provisión de técnicas electrónicas de búsqueda, acceso o recopilación de datos o de enlaces a otros espacios de la Red.

[63]Anexo a) de la LSSIyCE que reproduce el contenido del art. 2 de la Directiva 2000/31/CE. Se establece la remisión a la regulación de la responsabilidad civil, penal y administrativa del ordenamiento jurídico (art. 13 de la LSSIyCE).

[64] Recogido en los arts. 14 a 17 de la LSSIyCE y arts. 12 a 14 de la Directiva 2000/31/CE.

efectivo de que la actividad o la información a la que remite o recomienda es ilícita o que lesiona bienes o derechos de un tercero susceptibles de indemnización o, si lo tiene, no actúa con diligencia debida para suprimir o inutilizar el enlace correspondiente[65].

Por tanto, el motor de búsqueda no será en principio responsable porque no está obligado a supervisar la información que indexa lícitamente para difundirla a posteriori[66]. Lo que hace concluir que se reconoce como responsable al *webmaster* que alberga la red social en cuestión[67].

A fin de poder determinar un nivel correcto de seguridad para el usuario de la red social, en la práctica se va a recurrir al denominado 'derecho al olvido'. Entendido como la facultad del usuario de oponerse al tratamiento de la información personal que se está realizando y a su cancelación para que no sea difundida en futuras ocasiones[68]. Por tanto, el usuario tiene la opción de ejercitar dichos derechos ante el responsable del tratamiento. En concreto, el derecho de cancelación de los datos que le pertenecen y que incluyó en el perfil de la red social[69] o el derecho de oposición al tratamiento[70]. El primero de ellos significa que la información personal va a ser bloqueada por parte del responsable. Aunque es posible que los datos se mantengan *on line* por si en futuras ocasiones se decide volver a activar el perfil personal. Además la información del usuario, como se ha previsto, se suele ofrecer a terceros como los buscadores

[65] Art. 17 de la LSSIyCE. La expresión *conocimiento efectivo* hace referencia a los supuestos en los que *un órgano competente haya declarado la ilicitud de los datos, ordenado su retirada o que se imposibilite el acceso a los mismos, o se hubiera declarado la existencia de la lesión, y el prestador conociera la correspondiente resolución, sin perjuicio de los procedimientos de detección y retirada de contenidos que los prestadores apliquen en virtud de acuerdos voluntarios y de otros medios de conocimiento efectivo que pudieran establecerse*.

[66] Art. 15 de la Directiva 2000/31/CE. Como ocurre en el Procedimiento de la Agencia Española de Protección de Datos (TD 00249/2011), la cual recibe la reclamación de un sujeto contra las entidades *Google* y *Yahoo* por no haberse atendido su derecho de oposición al tratamiento de la información de carácter personal y de cancelación de a misma. La Agencia en su Resolución R/01545/2011 desestima la reclamación porque se considera que los prestadores de servicios de búsqueda no son responsables del tratamiento. Distinto resulta el planteamiento del Procedimiento de la Agencia Española de Protección de Datos (TD 0139/2010), la cual recibe la reclamación de una madre contra una productora y una cadena de televisión, una red social y un buscador que ejercitó su derecho de cancelación de la voz e imágenes de su familia. En particular, de su hijo menor de edad. En este caso, la Agencia resuelve (R/00668/2011) estimando la reclamación presentada contra la red social y el buscador por el trato vejatorio e injurioso realizado. Pero desestima las pretensiones efectuadas contra las otras dos entidades televisivas.

[67] Como se determina en el *Dictamen 5/2009*, de 12 de junio de 2009, del Grupo de Trabajo 29, *op.cit.,* pág. 5.

[68] Tal y como dispone el art. 14 y Cdo. 45 de la Directiva 95/46/CE.

[69] Arts. 16 de la LOPD y 31 del RLOPD.

[70] Arts. 17 de la LOPD y 34 del RLOPD.

electrónicos para que la indexen. En este planteamiento se exige que el responsable del tratamiento esté obligado a notificarle al tercero la cancelación de la misma. Por su parte, también puede ejercer el derecho de oposición con la pretensión de que no se traten los datos de carácter personal o que se cese en dicho tratamiento, según los términos de la norma. La cual prevé que se podrá ejercer esta facultad por razón del tratamiento y de manera justificada, sin que ello le reporte coste económico alguno.

En definitiva, corresponde al usuario que es el titular de su perfil ejercer el derecho de cancelación y eliminación de la información que consta a su nombre. A efectos de que el responsable del espacio lo ejecute haciendo las modificaciones que fueran necesarias para ello. Lo que traería como consecuencia, además, que se anulase la indexación que hubieran hecho los buscadores.

En otro orden, pero derivado de lo anterior, el prestador que ofrece la red social no sólo ha de facilitar el correcto funcionamiento de la misma desde el punto de vista técnico, sino también respetará los presupuestos en materia de protección de datos personales. Esto es, ha de atender al ejercicio de los derechos del sujeto, cancelando su perfil cuando corresponda y eliminando los datos e información que el afectado hubiera previsto en la red social. A ello hay que añadir que lo adecuado para la protección de los usuarios de las redes sociales es que se limite la indexación en la *política de privacidad* de la red social por defecto y que sólo en el caso de que el usuario lo hubiera consentido expresamente se pueda llevar a cabo por parte de los motores de búsqueda.

Por último, recordamos que si el ejercicio de los derechos no fueran atendidos por el responsable del tratamiento, el afectado puede presentar su reclamación a la Agencia de Protección de Datos al objeto de que ésta analice si procede o no la negativa del responsable. Y, en su caso, imponga la sanción que corresponda por la vulneración de derechos. En caso contrario, el sujeto que resulte afectado tiene la opción de acudir a la jurisdicción civil para solicitar la reparación de los daños ocasiones o a la vía contencioso–administrativa para interponer el recurso oportuno contra la resolución de la Agencia de Protección de Datos.

IV. Consideraciones finales

La información de los usuarios en el ámbito electrónico tiene una importante trascendencia, pues las entidades tratan de obtener datos sobre los mismos con el fin de conseguir captar su atención e intentar que accedan a sus espacios electrónicos y, en última instancia, que realicen transacciones *on line*.

La utilización de las redes sociales electrónicas por parte de los usuarios ha supuesto un nuevo entorno de comunicación no sólo para ellos, sino también para que las entidades del mercado virtual se publiciten y tengan una interacción con los usuarios. Si bien, a pesar de las ventajas que su uso reporta, no es menos cierto que también se han planteado inconvenientes desde la óptica jurídica. En particular, en lo que respecta a la protección del derecho a la intimidad y a los datos de carácter personal de los sujetos. Los cuales, en la mayor parte de las ocasiones, desconocen las técnicas que se pueden emplear en las redes sociales para hacer un seguimiento de la navegación de los mismos y, en su caso, el destino y tratamiento de la información que han facilitado y que forma parte de su esfera privada o de la de terceros.

La necesidad de garantizar la seguridad en el ámbito electrónico nos ha llevado a abordar, en primer término, las garantías que el ordenamiento ofrece a los usuarios en cuanto a los datos que le pertenecen y la manera en la que pueden ser atendidas por parte del prestador que ofrece el servicio de redes sociales. Siendo esencial, en este sentido, el contenido de la *política de privacidad* o del *aviso legal* que se pone a disposición de los usuarios que van a registrarse en una red social determinada. Pues, en base a dicho contenido, se va a conseguir incrementar la confianza de los sujetos en los nuevos medios de comunicación habilitados por la implementación de la telemática.

Tras ello, se han planteado dos de los problemas esenciales que surgen en este ámbito en relación con la recopilación y posterior tratamiento de información de carácter personal que concierne a los sujetos sin que ellos tengan conocimiento, ni lo hubieran autorizado. Por cuanto consideramos que la concienciación y formación a este respecto va a resultar básica para que los usuarios actúen en el entorno electrónico con diligencia y ello impida, en ciertos casos, intromisiones en su ámbito personal[71]. De un lado, se ha valorado el establecimiento de programas u otras técnicas informáticas que recopilan información y datos de los usuarios cuando se conectan a la Red y que van a destinarse a diversas finalidades; y, de otro, la necesidad de que el usuario que pretenda darse de baja de una red social ejercite determinados derechos recogidos en la normativa sobre protección de datos a efectos de que la información que facilitó se elimine del entorno electrónico.

Pese a lo analizado, somos conscientes de que se trata de una materia que va evolucionando, lo que hace suponer que aparezcan

[71] A este respecto, pueden consultarse las recomendaciones previstas en el 'Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online', *op.cit*., págs. 147-172, en particular págs. 166-172.

nuevos problemas jurídicos en relación con la seguridad de las redes electrónicas. En especial, en lo que concierne a la tutela de la intimidad de los usuarios y a la protección de los datos personales de los que es titular y que habrán de ser analizados.

V. Bibliografía

ALONSO MARTÍNEZ, Carlos, *Protección de datos de carácter personal. El consentimiento en entidades financieras*, Madrid, 2002.

ARENAS RAMIRO, Mónica, *El derecho fundamental a la protección de datos personales en Europa*, Valencia, 2006.

CAMPUZANO TOMÉ, Herminia, *Vida privada y datos personales*, Madrid, 2000.

CASTILLO JIMÉNEZ, Cinta, 'Protección del derecho a la intimidad y uso de las nuevas tecnologías de la información', *Anuario Jurídico sobre la Sociedad de la Información, Derecho y Conocimiento*, vol. I, 2001, págs. 35-48.

DAVARA RODRÍGUEZ, Miguel Ángel, *La protección de los intereses del consumidor ante los nuevos sistemas de comercio electrónico, Estudios y Documentación*, núm. 8, Madrid, 2000.

FERNANDO MAGARZO, Mª del Rosario, 'La protección de datos personales en el ámbito de la publicidad', *Revista de la Asociación de Autocontrol de la Publicidad*, núm. 77, julio/agosto, 2003, págs. 28-34.

FREIXAS GUTIÉRREZ, Gabriel, *La protección de los datos de carácter personal en el derecho español*, Barcelona, 2001.

GUERRERO PICÓ Mª. Carmen, *El Impacto de Internet en el Derecho Fundamental a la Protección de Datos de Carácter Personal,* Pamplona, 2006.

ILLESCAS ORTIZ, Rafael, 'La firma electrónica y el Real Decreto Ley 14/1999, de 17 de septiembre', *Derecho de los Negocios*, núm. 109, 1999, págs. 1-14.

MADRID PARRA, Agustín, 'Seguridad, pago y entrega en el Comercio Electrónico', *Revista de Derecho Mercantil*, núm. 241, julio/septiembre, 2001, págs. 1189-1263.

MARTÍNEZ NADAL, Apolonia, *Comercio electrónico, firma digital y autoridades de certificación*, 3ª edic., Madrid, 2001 y *Comentarios a la Ley 59/2003 de Firma Electrónica*, Madrid, 2004.

MORALES PRATS, Fermín, 'Internet: riesgos para la intimidad', en AA. VV. *Cuadernos de Derecho Judicial, Internet y Derecho Penal,* 2002, Madrid, págs. 63-82.

MORÓN LERMA, Esther*, Internet y Derecho Penal: hacking y otras conductas ilícitas en la Red,* 2ª edic., Pamplona, 2002.

MURILLO DE LA CUEVA, Pablo Lucas, 'La protección de los datos personales ante el uso de la informática', *Anuario de Derecho Público y Estudios Políticos*, núm. 2, 1989-1990, págs. 170-172.

PIÑAR MAÑAS, José Luis, 'Consideraciones introductorias sobre el derecho fundamental a la protección de datos de carácter personal', *Boletín del Ilustre Colegio de Abogados de Madrid*, núm. 35, 3ª época, febrero, 2007, págs. 11-44.

RIBAS ALEJANDRO, Javier, 'Riesgos legales en Internet. Especial referencia a la protección de datos personales', en AA. VV. (Coords. MATEU DE ROS/ CENDOYA MÉNDEZ DE VIGO), *Derecho de Internet (Contratación electrónica y Firma digital)*, Navarra, 2000, págs. 143-164 y *Aspectos Jurídicos del Comercio Electrónico en Internet,* 2ª edic., Navarra, 2003.

SERRANO PÉREZ, Mª. Mercedes, *El derecho fundamental a la protección de datos. Derecho español y comparado*, Madrid, 2003.

VAZQUEZ RUANO, Trinidad, 'Una nueva proyección del derecho a la intimidad. La autodeterminación informativa', *Revista Crítica de Derecho Privado*, núm. 5, 2008, págs. 49-72 y *La protección de los destinatarios de las comunicaciones comerciales electrónicas*, Madrid, 2008.

VELÁZQUEZ BAUTISTA, Rafael, *Derecho de las Tecnologías de la Información y las Comunicaciones (T.I.C)*, Madrid, 2001.