REDES SOCIALES ONLINE: FUENTES DE ACCESO PÚBLICO O FICHEROS DE DATOS PERSONALES PRIVADOS

(Aplicación de las Directivas de protección de datos y privacidad en las comunicaciones electrónicas)

ROSA MARÍA GARCÍA SANZ

SUMARIO

© UNED. *Revista de Derecho Político*
N.º 81, mayo-agosto 2011, págs. 101-154

Fecha recepción: 20.04.2011
Fecha aceptación: 20.05.2011

REDES SOCIALES ONLINE: FUENTES DE ACCESO PÚBLICO O FICHEROS DE DATOS PERSONALES PRIVADOS

(Aplicación de las Directivas de protección de datos y privacidad en las comunicaciones electrónicas)

POR

ROSA MARÍA GARCÍA SANZ

Profa. Titular Derecho de Constitucional
Universidad Complutense

INTRODUCCIÓN

Los sitios Internet de redes sociales han sido definidos por el Grupo de Trabajo sobre Protección de Datos del Artículo 29[1]como «plataformas de comunicación en línea que permiten a los individuos crear redes de usuarios que comparten intereses comunes. En sentido jurídico, las redes sociales son servicios de la sociedad de la información, según se definen en el artículo 1, apartado 2, de la Directiva 98/34/CE, modificada por la Directiva 98/48/CE»[2]. El estudio sobre

[1] GRUPO DE TRABAJO CREADO POR EL ARTÍCULO 29 de la Directiva 95/46/CE, es un organismo de la UE, con carácter consultivo e independiente, para la protección de datos y el derecho a la intimidad. Sus funciones se describen en el artículo 30 de la Directiva 95/46/CE y el artículo 15 de la Directiva 2002/58/CE.

[2] Dictamen 5/2009 sobre las redes sociales en línea. Adoptado el 12 de junio de 2009. 01189/09/ES. W163. Disponible en: http://ec.europa.eu//justice_home/fs/privacy/index_en.htm

privacidad de los datos y la seguridad de la información en las redes sociales online, realizado por el Instituto Nacional de Tecnologías de la Comunicación y la Agencia Española de Protección de Datos, considera que «las redes sociales online son servicios prestados a través de Internet que permiten a los usuarios generar un perfil, desde el que hacer públicos datos e información personal y que proporcionan herramientas que permiten interactuar con otros usuarios y localizarlos en función de las características publicadas en sus perfiles»[3]. También en el llamado *Memorandum* de Roma[4] se ha reflexionado sobre la naturaleza de estos servios online, y donde se explica como las fronteras entre el espacio de lo privado y lo público se mueven: pues los datos personales sobre los individuos se convierten en públicos y globales, a iniciativa propia, disponible la información de una manera y en unas cantidades sin precedentes[5]. Estos y otros informes, como el de ENISA[6] o el de la Conferencia Internacional de Madrid[7], sin olvidar las distintas resoluciones y decisiones en el ámbito de UE[8] sobre los servicios de las redes sociales, ayudan a abordar y acotar el significado de las redes sociales online desde una perspectiva jurídica. Dada la autoridad de los titulares de tales documentos, que aún sin valor jurídico vinculante sí tienen gran influencia, sus posiciones resultan terreno firme en el que asentar un nuevo estudio.

Aunque existe toda una tipología y topología de redes sociales[9], es posible abstraer unas características comunes a todas ellas que, en definitiva, nos sitúen

---

[3] Estudio realizado por INTECO y la AGENCIA DE PROTECCIÓN DE DATOS DE ESPAÑA en 2009. Disponible en: www.inteco.es, y también en, www.agpd.es. Pág. 38.

[4] Informe del INTERNATIONAL WORKING GROUP ON DATA PROTECTION IN TELECOMMUNICATIONS. «Report and Guidance on Privacy in Social Network Services». 675.36.5. Roma, 4 de Marzo de 2008. Disponible en http://www.berlin-privacy-group.org

[5] Ibid. Pág.1 «*At the same time, social networking services seem to be pushing at the boundaries of what societies see as a persons' individual space: Personal data about individuals became publicly (and globally) available in an unprecedented way and quantity, especially including huge quantities of digital piectures and videos».*

[6] EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY (ENISA). Position Paper No.1. *Secutity Issuess and Recommendations for Online Social Networks.* October 2007.

[7] 31ª Conferencia Internacional de Autoridades de Protección de Datos y privacidad, reunida en Madrid el día 5 de noviembre de 2009. Disponible en: http://www.agpd.es

[8] *Resolution on Privacy Protection in Social Networks Services.* 30 th. Internacional Conference of Data Protection and Privacy Commissioners. Strasbourg, 17 de October 2008.

Recomendación del CONSEJO DE MINISTROS DEL CONSEJO DE EUROPA, REC (2010)13, 23 de nov. 2010*, «sobre protección de las personas en relación con el procesamiento automatizado de datos personales para la creación de perfiles».*

[9] HUETE NOGUERAS, J. (2010). «Comentarios en torno al origen de las redes sociales y algunos aspectos del tratamiento de los datos de carácter personal aportados por las mismas», *Revista Otrosí.*, núm. 4, Octubre de 2010. 5ª Epoca, p. 19.

en su naturaleza común[10], sin perjuicio de las oportunas consideraciones particulares. Igualmente, los riesgos tecnológicos para la privacidad o intimidad[11] no se limitan a la problemática de los servicios de las redes sociales online, sino que se extienden a los blogs, webs interactivas, las etiquetas RFID, la computación ubicua, por poner algún ejemplo; sin embargo, la popularidad y el crecimiento imparable de las mismas, que se agranda con la telefonía móvil y otros artefactos electrónicos, las pone en un punto de mira preferente. No cabe duda que estos servicios deben respetar los derechos y libertades fundamentales de los usuarios, que no sólo ven su derecho a la protección de datos personales en riesgo, y su privacidad misma, sino también otros derechos fundamentales. Aunque, sin duda, es este nuevo derecho de última generación el que *prima facie* se ve más amenazado, precisamente por la naturaleza misma de la red social, como colección de datos personales.

Se insiste sobre la naturaleza privada de estas plataformas, donde los particulares establecen relaciones personales con la familia, amigos o conocidos, basadas en la confianza y en la voluntariedad de los datos e información que aportan, pero no se atiende lo suficiente a su papel de medio de comunicación social, que, por otra parte, es indudable, si se observa la realidad actual, y la función indiscutible de estas redes en la libertad de expresión e información, con un gran impacto político social. E incluso, dando un paso más atrevido, en cierta manera, se pueden entender como nuevas «guías de abonados» de los servicios de comunicación electrónica. Es por ello que el objeto del presente trabajo pretenda

[10] El dictamen W163 del GRUPO DE TRABAJO DEL ART. 29, ya citado, subraya las siguientes:

— «los usuarios deben proporcionar datos personales para generar su descripción o perfil;

— los SRS(servicios de redes sociales) proporcionan también herramientas que permiten a los usuarios poner su propio contenido en línea (contenido generado por el usuario como fotografías, crónicas o comentarios, música, vídeos o enlaces hacia otros sitios);

— las «redes sociales» funcionan gracias a la utilización de herramientas que proporcionan una lista de contactos para cada usuario, con las que los usuarios pueden interactuar.

Los SRS generan la mayoría de sus ingresos con la publicidad que se difunde en las páginas web que los usuarios crean y a las que acceden. Los usuarios que publican en sus perfiles mucha información sobre sus intereses ofrecen un mercado depurado a los publicitarios que desean difundir publicidad específica y basada en esta información», p. 5.

[11] Aunque las Directivas e incluso la legislación parecen usar ambos términos como intercambiables, hay que advertir que poseen un contenido jurídico diferenciado y específico, aunque con zonas comunes, pues todo lo íntimo es privado pero no al revés. Véase, por ejemplo: PARDO LÓPEZ, M. M. (2007). «Intimidad personal, protección de datos sanitarios e intromisiones ilegítimas: Una proyección hipotética de la doctrina *Tarasoff* sobre el ordenamiento jurídico español», en *Anales de Derecho.,* Universidad de Murcia, núm. 25, 2007, págs. 181-214.

una mirada, sin prejuicios jurídicos, sobre estas redes sociales online, conforme a las Directivas de protección de datos personales y privacidad, que identifique hasta dónde llega su naturaleza de fichero privado o base de datos personales y hasta dónde la de fuente pública de datos accesibles al público, extrayendo las consecuencias consiguientes para su posible regulación o la aplicación de la ley.

1. ÁMBITO DE APLICACIÓN Y SERVICIOS AFECTADOS: INCLUSIÓN DE LAS REDES SOCIALES.

El nuevo paquete legislativo que ha venido a modificar el actual marco regulador de la UE de las redes y los servicios de comunicaciones electrónicas[12], incluye en la Directiva 2009/136/CE algunos cambios de calado respecto a la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (llamada Directiva sobre privacidad y comunicaciones electrónicas), a la que modifica. El considerando 51 de la nueva Directiva reza así: «La Directiva 2002/58/CE (Directiva sobre la privacidad y las comunicaciones electrónicas) armoniza las disposiciones de los Estados miembros necesarias para garantizar un nivel equivalente de protección de los derechos y las libertades fundamentales y, en particular, del derecho a la intimidad y a la confidencialidad, en lo que respecta al tratamiento de los datos personales en el sector de las comunicaciones electrónicas… garantizar que los equipos terminales estén fabricados de manera que protejan los datos personales y la intimidad, estas (normas) deben respetar el principio de neutralidad respecto a la tecnología».

Habida cuenta que estas Directivas en su tenor literal se aplican a la redes públicas y a los servicios de comunicaciones electrónicas a través de las mismas, y que éstos a su vez pueden constituir servicios de la sociedad de la

[12] Directiva 2009/140/CE del Parlamento Europeo y del Consejo de 25 de noviembre de 2009, por la que se modifican la Directiva 2002/21/CE relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/19/CE relativa al acceso a las redes de comunicaciones electrónicas y recursos asociados, y a su interconexión, y la Directiva 2002/20/CE relativa a la autorización de redes y servicios de comunicaciones electrónicas.

Y la Directiva 2009/136/CE del Parlamento Europeo y del Consejo de 25 de noviembre de 2009, por la que se modifican la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas y el Reglamento (CE) nº. 2006/2004 sobre la cooperación en materia de protección de los consumidores.

información[13], parece aconsejable examinar previamente el encaje de los servicios de las redes de sociales en estas categorías, con el fin de delimitar las normas comunitarias y nacionales que le son aplicables en la materia. No hay que olvidar que en el proceso de elaboración del nuevo paquete de Directivas citado, concretamente en relación a la Directiva sobre privacidad y comunicaciones electrónicas, la cuestión del «ámbito de aplicación y servicios afectados» fue uno de los centros de debate de más disenso[14]. Superada la terminología **de sector y servicios de telecomunicaciones**, «en primer lugar, fruto de los avances tecnológicos y de la convergencia, las tradicionales telecomunicaciones han dejado paso a **los servicios de comunicaciones electrónicas**, en un avanzado concepto de transmisión donde convergen los sectores audiovisual y de las telecomunicaciones con las actuales posibilidades tecnológicas. En segundo lugar, los **servicios de la sociedad de la información**, como espacio jurídico propio en el que encuentran cabida específicos servicios de transmisión y de contenido. **Y formando parte de unos y de otros, en una posición de auténtico protagonismo, el universo virtual de Internet**»[15], es preciso partir de una clarificación de todos estos conceptos y términos en la legislación comunitaria y española, con el fin de delimitar estas categorías[16] y examinar si existe cabida en ellas para los servicios de las redes sociales.

[13] Como es el caso del servicio de acceso a Internet u otros servicios de transmisión.

[14] Véanse los Dictámenes del SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS: Dictamen del Supervisor Europeo de Protección de Datos sobre la Propuesta de Directiva del Parlamento Europeo y del Consejo por la que se modifica, entre otras, la Directiva 2002/58/CE, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas. (2008/C181/01). Y el Segundo Dictamen del Supervisor Europeo de Protección de Datos sobre la revisión de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio de 2002 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas). (2009/C128/04).

[15] BALLESTEROS MOFFA, L.A. (2005). *La privacidad electrónica. Internet en el centro de protección*., Tirant lo Blanch, Valencia, 2005, p. 207.

[16] Ibid., p. 237. Ya se manifestó respecto a la modificada Directiva 2002/58/CE, que «que la protección dispensada por la vigente Directiva de protección de datos en el ámbito de las comunicaciones electrónicas, además, no se halla siquiera condicionada por los límites materiales que pudieran derivarse de los marcos reguladores o de las categorías sustantivas de los servicios de comunicaciones electrónicas y de la sociedad de la información, pues si bien esta disposición se incardina dentro del bloque comunitario relativo a las redes y servicios de comunicaciones electrónicas, que excluye todos aquellos servicios de la sociedad de la información que no son de transmisión, su ámbito protector también se extiende a los mismos, sin hallarse tampoco limitada por los estrictos requisitos conceptuales de tal categoría».

1.1. Servicios de la Sociedad de la Información

Es pacífica la inclusión de los servicios de las redes sociales en la categoría jurídica de «servicios de la sociedad de la información», y parece encajar en la definición que figura en el artículo 1 de la Directiva 98/34CE del Parlamento Europeo y del Consejo, de 22 de junio de 1998[17]. Y, en consecuencia directa, caen dentro del ámbito de aplicación de la Directiva de Servicios de la Sociedad de la Información[18] y de su implementación en España por la Ley del Comercio electrónico[19]. Y éstas, a su vez, en materia de protección de datos, remiten a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las Personas Físicas en lo que respecta al Tratamiento de Datos Personales y a la libre Circulación de estos datos; y a la Ley Orgánica 15/1999, de 13 de Diciembre, Protección de Datos de Carácter Personal[20], respectivamente.

1.2. Servicios de comunicaciones electrónicas

La Directiva 2002/21/CE relativa a un marco regulador común de las redes y de los servicios de comunicaciones electrónicas, define en su artículo 2º. c) el **servicio de comunicaciones electrónicas**: «el prestado por lo general a cambio de una remuneración que consiste, en su totalidad o principalmente, en el transporte de señales a través de redes de comunicaciones electrónicas…pero no de los servicios que suministren contenidos transmitidos mediante redes y servicios de comunicación electrónica, o ejerzan control editorial sobre ellos; quedan excluidos, asimismo, los servicios de la sociedad de la información definidos en el artículo 1 de

[17] Directiva 98/34/CE, del Parlamento Europeo y del Consejo, por la que se establece un procedimiento de información en materia de las normas y reglamentación técnica y de las reglas relativas a los servicios de la sociedad de la información. En su art. 1.2: «**servicio de la sociedad de la información, es decir, todo servicio prestado normalmente a cambio de una remuneración, a distancia, por vía electrónica y a petición individual de un destinatario de servicios».**

[18] Directiva 2000/31/CE, de 8 de junio, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, y en particular el comercio electrónico en el mercado interior.

[19] Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y del Comercio electrónico (LSSI-CE).

[20] Desarrollada por el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica de Protección de Datos (RDLOPD).

la Directiva 98/34/CE que no consistan, en su totalidad o principalmente, en el transporte de señales a través de redes de comunicación electrónica». Asimismo, el nuevo artículo 3 de la modificada Directiva 2002/58/CE[21] (Directiva sobre privacidad y comunicaciones electrónicas) establece como **servicios afectados** lo siguiente: «la presente Directiva se aplicará al tratamiento de datos personales en relación con la prestación de servicios de comunicaciones electrónicas disponibles al público en las redes públicas de comunicaciones de la Comunidad, incluidas las redes públicas de comunicaciones que den soporte a dispositivos de identificación y recopilación de datos». Y la nueva redacción del art. 2, apartado d) de la Directiva marco[22] define lo que a efectos de las normas comunitarias se entiende por «**red pública de comunicaciones**»: «una red pública de comunicaciones electrónicas que se utiliza, en su totalidad o principalmente, para la prestación de servicios de comunicaciones electrónicas disponibles para el público y que soporta la transferencia de información entre puntos de terminación de red».

Los servicios de las redes sociales online se soportan y realizan a través de servicios de comunicaciones electrónicas disponibles al público en las redes públicas, pero no encajan en la definición legal de servicio de comunicación electrónica. Sin embargo, algunos de los artículos de la Directiva sobre privacidad y comunicaciones electrónicas se aplican a los servicios de la sociedad de la información[23], en cuyo concepto se subsume el de la red social online, porque así lo ha querido el legislador. Es más, cuando en el artículo 1.1[24] se acota el ámbito de aplicación y objetivo, su tenor literal es lo suficientemente generoso para que se extiendan sus normas al «tratamiento de los datos personales en el **sector de las comunicaciones electrónicas**, así como la libre circulación de tales datos y de los equipos y servicios de comunicaciones electrónicas en la Comunidad». Nótese que al utilizar ese lenguaje, permite que no se agote su aplicación sólo en los «servicios de comunicación electrónica» definidos legalmente, sino que deja margen para que se observen otros servicios o actividades, siempre que se sustancien en el **sector** de las comunicaciones electrónicas. De ahí que algunas de sus disposiciones son de clara aplicación a los servicios de la sociedad de la información, y por vía interpretativa incluso se podría ir más allá.

[21] Modificación mediante la citada Directiva 2009/136/CE del Parlamento Europeo y del Consejo de 25 de noviembre de 2009.

[22] Directiva 2009/140/ CE del Parlamento Europeo y del Consejo de noviembre de 2009, que introduce las modificaciones.

[23] Que no sean de transmisión.

[24] Nueva redacción dada por la Directiva 2009/136/CE, ya citada anteriormente.

Recordar nuevamente que el Supervisor Europeo en sus Dictámenes para la modificación de la Directiva, ya citados, tuvo uno de sus caballos de batalla en el ámbito de aplicación y los servicios afectados[25]. Y reiteró su desacuerdo al no ampliarse su ámbito de aplicación y los servicios afectados a los de las redes privadas o semipúblicas. O a todos los servicios de la sociedad de la información, y a incluirse, por tanto, en algunas de las medidas, no sólo a los proveedores de servicios de comunicaciones electrónicas disponibles al público sino también a los prestadores de servicios de la sociedad de la información, en redes públicas y privadas o, incluso, en las muy numerosas semipúblicas (o semiprivadas, si se quiere). Así, por ejemplo, en el apartado 26 del Segundo Dictamen manifiesta «en este contexto, el SEPD (Supervisor Europeo de Protección de datos) desearía recordar los siguientes: i) No hay obstáculo legal alguno para incluir a agentes distintos de las PSCEP (proveedores de servicios de comunicaciones electrónicas disponibles al público) en el ámbito de aplicación de determinadas disposiciones de la Directiva. El legislador comunitario goza de plena discrecionalidad a este respecto. ii) En la Directiva en vigor sobre la intimidad y las comunicaciones electrónicas existen precedentes de aplicación a entidades distintas de las PSCEP»[26]. Se refiere el SEPD a los prestadores de servicios de la sociedad de la información (PSSI).

Si bien es cierto que, como lamenta reiteradamente el SEPD, desde 2003 la aplicación de las disposiciones de la Directiva sobre intimidad y comunicaciones electrónicas, —y un análisis detallado de la misma lo ha mostrado— que algunas disposiciones distan de ser claras, con lo que provocan inseguridad jurídica y dificultan su cumplimiento[27], también hay que reconocer que «en una concreción de los principios de la Directiva 95/46/CE, con la incorporación al art. 5 del fundamental apartado 3, en los amplios términos referidos (no limitados a la categoría formal de los servicios de la sociedad de la información), junto a los correspondientes considerandos vigésimo cuarto y vigésimo quinto, alusivos a los denominados programas espía (*spyware)*, *web bugs*[28], identificadores ocultos u otros dispo-

[25] En la parte II.1, punto 1.4, del Dictamen C181/4, en 2008, manifestaba: «Una cuestión principal en la actual Directiva sobre intimidad y comunicaciones electrónicas es la de su ámbito de aplicación. La Propuesta contiene algunos elementos positivos que sirven para definirlo y aclararlo, sobre todo en lo tocante a los servicios a los que afecta la Directiva, de los que trataremos en punto i). Desgraciadamente, las modificaciones propuestas no resuelven todos los problemas actuales. Como veremos en el punto ii), las modificaciones no persiguen, lamentablemente, ampliar el ámbito de aplicación de la Directiva de modo que incluya los servicios de comunicaciones electrónicas de redes privadas».

[26] Dictamen 2009/C 128/04, ya citado anteriormente.

[27] Primer Dictamen, ya citado, apartado 12 de la primera parte.

[28] BALLESTEROS MOFFA, L.A., *La privacidad electrónica*., o.c., p. 240.

sitivos análogos, como los conocidos chivatos o *cookies*»[29], han supuesto un avance. Cuestiones que han sido ampliadas y reformadas a la luz de la evolución tecnológica y de las prácticas observadas. Con todo, de nuevo se ha perdido la oportunidad de regular de forma integral y coherente el tratamiento de los datos personales en relación con la prestación de servicios a través de las redes y los servicios públicos de comunicaciones, como son los servicios de la sociedad de la información, o en otras palabras, los servicios que transmiten contenidos mediante el uso de redes y servicios de comunicaciones electrónicas disponibles al público.

De lo cual se extrae, en materia de protección de datos y privacidad, para los servicios de las redes sociales online, que habrá que atender siempre a la Directiva 95/46/CE general de protección de datos y a la Directiva de los Servicios de la Sociedad de la Información, y siempre que sea posible, a aquellos artículos que sean aplicables de la Directiva de las comunicaciones electrónicas y privacidad[30], en los que en legislador ha querido dar entrada a otros servicios, como los servicios de la sociedad de la información. De manera que en algunos casos estará obligado y responderá el prestador de servicio de la red social, en otros el proveedor de servicio de Internet, y en otras situaciones pueden responder conjuntamente, conforme a los términos de la ley. También puede ocurrir que el proveedor de servicio de Internet o comunicaciones electrónicas disponibles al público coincida en la misma persona del prestador de servicio de la red social online. E incluso, como se verá después, el mismo usuario podría verse en la situación de responder del tratamiento del conjunto de datos (e informaciones) que reúne en su espacio de red social. Una falta de certeza en cuanto a la disposición a aplicar o la persona que debe responder, puede provocar inseguridad jurídica, que perjudicaría principalmente a los usuarios en su derecho fundamental a la protección de datos personales[31].

[29] Ibid. p. 240.

[30] Teniendo en cuenta que esta Directiva exige, en primer lugar, el cumplimiento de la Directiva 95/46/CE, que contiende la regulación general y básica. Y que, además, como norma especial atiende a aspectos específicos y concretos de las comunicaciones electrónicas, cuyas disposiciones tendrán prioridad en esta materia.

[31] Derecho fundamental de configuración jurisprudencial, que comenzó con Sentencias como la STC254/1993 y culminó con la STC 292/2000, cuyo fundamento jurídico quinto define un nuevo derecho fundamental dotándolo de plena autonomía respecto a la intimidad. Por otra parte, la jurisprudencia del Tribunal Europeo de Derechos Humanos ha extendido la aplicación del artículo 8 CEDH con un concepción muy amplia de la vida privada y familiar que alcanza el reconocimiento del derecho a la protección de datos en los términos del Convenio Europeo núm., 108. En el marco de la Unión Europea el artículo 8 de la Carta Europea de Derechos Fundamentales reconoce de manera específica el derecho a la protección de datos como derecho autónomo del derecho a la vida privada. Derecho que se encomienda su tutela a las autoridades independientes y cuyo principio también se recoge en el artículo 286 del Tratado de la Comunidad Europea.

2. EL PRINCIPIO GENERAL DE ACCESO A LAS FUENTES PÚBLICAS VS. PRINCIPIO GENERAL DE PROTECCIÓN Y PRIVACIDAD DE LOS DATOS PERSONALES

El principio de acceso general a las fuentes de información públicas tiene su más pleno sentido cuando se trata de la Administración pública del Estado. El artículo 105.b) de la Constitución Española establece que la «la ley regulará[32] el acceso de los ciudadanos a los archivos y registros administrativos, salvo en lo que afecte a la seguridad y defensa del Estado, la averiguación de los delitos y la intimidad de las personas». **El acceso a las fuentes de información del Estado** se entiende como un contrapeso[33] de la sociedad civil para controlar el poder del Estado[34], y cuya regulación jurídica no ha satisfecho, hasta el momento, las expectativas que se abrigaban[35]. Ahora bien, este **principio general entraña excepciones**, cuyos fundamentos están en el propio texto constitucional[36]: el interés general y el derecho a la intimidad de las personas, que en el ámbito de la protección de datos tienen una proyección bifronte: como uno de los fundamentos para la protección (la privacidad e intimidad) y como una excepción a la protección (el interés general). Es por ello que la Administración del Estado no escapa al sometimiento de la Ley Orgánica de Protección de Da-

---

Para una visión en conjunto de este derecho en Europea, véase: ARENAS RAMIRO, MÓNICA.(2006). *El Derecho Fundamental a la Protección de Datos Personales en Europa.*, Tirant lo Blanch, Valencia, 2006.

[32] Dando cumplimiento a este mandato constitucional, aunque de forma limitada e insuficiente, si se atienden a las diversas opiniones doctrinales: La Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones públicas y del Procedimiento Administrativo Común. Y más recientemente, la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.

[33] Entre otras funciones, pues forma parte del derecho a información del ciudadano y es absolutamente necesario pues se constituye, a su vez, en garantía institucional del derecho a la participación democrática. Sobre el llamado «derecho de acceso» y sus diversas interpretaciones, si como derecho autónomo o como parte del contenido del derecho a la información, véase por todos: GUICHOT, EMILIO. (2010). «Transparencia y acceso a la información en Derecho europeo y comparado», *Derecho Global*, Sevilla, 2010.

[34] PEREZ UGENA, MARIA Y ALVARO. (2002). «Implicaciones constitucionales de las nuevas tecnologías» en *Revista de Derecho Político.,* núm.54, UNED, 2002, pp. 186 y ss.

[35] Véase por todos: COTINO HUESO, L (2007). «Acceso a la información pública en la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos», en El *derecho de acceso a la información pública., Actas del Seminario Internacional Complutense*. Madrid, 27-28 junio 2007.

[36] Artículo 105 CE y en relación con el art. 103 CE.

tos de Carácter Personal[37], pero el **interés general que prima en sus actuaciones es causa de un gran elenco de excepciones al régimen general establecido** por la ley. El régimen jurídico de protección de datos personales es común para las Administraciones Públicas y para los particulares. No existe una norma propia y única para los tratamientos de datos personales llevados a cabo por los poderes públicos. No podría ser de otra manera ya que el objeto de esta Ley es garantizar y proteger las libertades públicas y los derechos fundamentales de las personal físicas, y especialmente su honor e intimidad personal y familiar, en lo que concierne al tratamiento de los datos personales —art.1 LOPD— y esta protección tiene una vocación universal. Las diferencias entre los ficheros públicos y privados se desgranan en el texto de la ley. Los ficheros públicos disponen de un conjunto de exclusiones en el ámbito de aplicación y de excepciones a los principios de protección de datos y a los derechos de los interesados».[38]

Ahora bien, la continua necesidad de armonización del principio de acceso a la información pública y el principio de protección de los datos personales no se produce sólo en el sector público o de las Administraciones públicas, sino también se impone en el sector privado o de los particulares. Y es por ello que tanto la LOPD (Ley Orgánica de Protección de Datos) como la normativa europea[39] re-

[37] Ni al régimen comunitario en materia de protección de datos personales, consecuentemente.

[38] TRONCOSO REIGADA, A. (2007). «La Protección de datos personales en las Administraciones Públicas», en *Revista Jurídica General. Boletín del Ilustre Colegio de Abogados de Madrid*., núm. 35, 3ª época, Febrero 2007, p. 267. De este mismos autor*:* (2010) *Comentario a la Ley Orgánica de Protección de datos de Carácter Personal*, Civitas, Madrid, 2010

Véanse por todos, y por citar algunos estudios representativos, pues la bibliografía aquí es muy númerosa: FERNÁNDEZ RAMOS, S. (1997). *El Derecho de acceso a los documentos administrativos*, Marcial Pons, Madrid, 1997; GUICHOT, E. (2007). «Acceso a la información en poder de la Administración y protección de datos personales», en *Revista de Administración Pública*, núm. 173, mayo-agosto, 2007, pp. 407-445. Y, FERNÁNDEZ SALMERÓN, M.Y VALERO TORRIJOS, J. (2005). «La publicidad de la información administrativa en Internet: implicaciones para el derecho a la protección de datos personales», en *Revista Aragonesa de Administración Pública*, núm. 26, 2005.

[39] En la Directiva 45/96/CE, en diferentes considerandos, como los considerandos 17, 37, 34, 39, 43, se explican las distintas excepciones a los derechos de los titulares, tanto si se aplican sólo al Estado o también a los particulares. En el articulado de la norma, los artículos 9, 11.2 y 13, principalmente, establecen estas excepciones o límites. En la Ley Orgánica española las excepciones dirigidas a los ficheros públicos se encuentran en los artículos 22 y 23. Y las referidas a los ficheros privados en los artículos 26, 27, 28, 29 y 30, que se refieren principalmente a las «fuentes de acceso público». Las excepciones que afectan a ficheros se a ambos tipos se encuentran en el artículo 6.2, 7.2, 7.3,8, y apartados 2 y 6 del art. 11.

cogen **un conjunto de excepciones a los principios y derechos** de los interesados que responden al interés general, —aunque con finalidades distintas a las previstas exclusivamente para la Administración General del Estado, y sin excluirla—, **los particulares** gozan **de una serie de excepciones por razones de investigación histórica, científica, estadística o informativas.** Entre ellas se encuentran las que la LOPD española denomina «fuentes accesibles al público»: se trata de una de las principales excepciones al consentimiento del titular de los datos, de forma que sin contar con éste se va a poder tratar en el sector privado determinados datos de carácter personal. La definición de las fuentes accesibles al público aparecen en la apartado j del artículo 3 de la LOPD y su regulación para los ficheros privados se encuentra en artículo 28 del mismo cuerpo legal.

2.1. El derecho a la protección de datos personales y sus excepciones: el interés general.

El usuario de una red social publica información personal en línea (el llamado perfil del usuario), a la que se añaden los datos que describen las acciones e interacciones del usuario con otras personas (todo lo que se muestra en su «pared»o enlaces a otros sitios, etc.,), por lo que es factible y hasta muy fácil crear un «retrato» muy preciso de los intereses y actividades del usuario. Es cierto que un gran número de **usuarios interactúan en un ámbito puramente personal**[40], con personas de su entorno familiar, de amigos o contactos domésticos, en definitiva, y se les podría aplicar la cláusula de exención respecto a su colección de datos. Pero también lo es que cada vez más **personas utilizan estas plataformas de una forma muy abierta, con fines profesionales, económicos, sociales, culturales o políticos**. E incluso las personas que en principio sólo tienen un objetivo de comunicación personal, puede ocurrir que permitan (o sin permitirlo) que su perfil y/o sus comunicaciones sean vistas o se tengan acceso por una gran mayoría de personas o sean de acceso público general. Pero aún más, se puede producir **la utilización y difusión de la información (datos) disponibles en la red social online con fines secundarios** y ajenos, **no buscados por el usuario**. Y ello tanto **por terceros desde dentro de la propia** red (por otros usuarios y hasta por los prestadores y proveedores de servicio) **como desde fuera de la red** (proveedores de software del sitio, personas que accedan me-

[40] Con lo que se podría aplicar en estos casos la exención de «actividades exclusivamente personales o domésticas» de los ficheros mantenidos por personas físicas. Art. 2.2 a) LOPD y en relación con la Directiva 45/96/CE.

diante interfaz, motores de búsqueda[41], *cookies,* etc…). Los datos personales publicados (e incluso los no publicados pero que generan las máquinas y los distintos mecanismos de software a partir de los usos y acciones del usuario) pueden ser utilizados con distintos fines, en particular, comerciales, y pueden representar grandes riesgos, como la usurpación de identidad, perdidas económicas o profesionales o de empleo, ataques a la integridad física, etc.

En principio, parece lógico que estos servicios y los prestadores de los mismos funcionen respetando los derechos y libertades del usuario, y por lo tanto cumpliendo, también, la normativa en materia de protección de datos personales y privacidad. Y aunque cabe esperar que los usuarios tengan la misma expectativa respecto a los datos que revelan, no siempre es así ni tiene por qué ser así. Los llamados «nativos digitales», especialmente, muestran unas actitudes y comportamientos en red que contradicen tales expectativas, y que mientras caigan dentro de los principios y derechos[42] establecidos en la legislación europea y nacional[43] no hay nada que objetar. **La cuestión que surge es si realmente se están o no ejercitando derechos[44] o si sencillamente la realidad de estas plataformas de comunidades virtuales se manifiesta resistente a la legis-**

[41] Las técnicas de «captcha» (Completely Automated Public Turing Test to tell Computer and Human Apart), no se emplean para evitar la indexación en motores de búsqueda. Se utilizan para evitar las suscripciones masivas automáticas o generalmente los ataques por denegación de servicio. Pero no hay que olvidar que todas son superadas y que por otra parte hay intereses comerciales que se imponen.

[42] Es decir, si el sujeto es libre de acceder a Internet y de integrase en estas redes y de libremente consentir en revelar estos datos, como de ejercitar el resto de los derechos que establecen las leyes de protección de datos personales (especialmente los derechos ARCO: derechos de acceso, rectificación, cancelación y oposición), nada hay que objetar. En este sentido, véase el Estudio sobre privacidad y redes sociales, ya citado, de la AGEPD y de INTECO. Lo principios de la protección de datos y los derechos de las personas están establecidos en los Títulos II y III de La Ley Orgánica de Protección de los datos Personales de 1999, que implementa la Directiva 95/46/CE, ya reiteradamente citadas ambas.

[43] Desde el punto de vista internacional se están haciendo esfuerzos para una protección global.

[44] No en balde este derecho se ha denominado en sus orígenes como «derecho a la autodeterminación informativa» haciendo alusión al poder de control y disposición que debe tener el individuo sobre sus datos e información personal.

Sobre los orígenes y construcción de este derecho véanse, por todos: LUCAS MURILLO DE LA CUEVA, P. (1999). «La Construcción del Derecho a la Autodeterminación Informativa», en *Revista de Estudios Políticos* (Nueva Epoca) Núm.104. Abril-Junio 1999. También, VILLAVERDE MENÉNDEZ, I. (1994). «Protección de datos personales, Derecho a ser informado y Autodeterminación Informativa del Individuo, a propósito de la STC 254/1993», *en Revista Española de Derecho Constitucional*. Año 14. Núm.41. Mayo-Agosto 1994.

lación en la materia, porque son simplemente «otra cosa»[45]. El cuestionamiento de conceptos en el mundo digital[46] no es nuevo, e incluso, afrontando los problemas en estos servicios de redes sociales, se llega a cuestionar el concepto mismo de «dato personal»[47]. Ahora bien, en tanto en cuanto, de una u otra manera, nos encontramos ante una colección de datos personales privados que responde a la definición de «fichero»[48], éstos atraen toda la protección de la ley y también ceden ante las excepciones que en la misma se imponen, por razones de interés público general[49]. El artículo 6.2 de LOPD dice: «No será preciso el consentimiento (para el tratamiento)[50] cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7 apartado 6 de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y

[45] El ya citado «Memorandum de Roma» desenmascara en su informe el mal entendimiento o la asunción equivocada de algunos términos o conceptos cuando se aplican a la Red o a los servicios de redes sociales concretamente. Por ejemplo, trasladar el concepto de «comunidad real» al de «comunidad virtual», o el término «social», que puede llevar al error de pensar que estamos ante recursos públicos libres, sin contrapartida de pago correspondiente. Respecto a las comunidades virtuales afirma: «*The misleading notion of "community": Many service providers claim that they are bringing communication structures from the «real» world into the cyberspace. Acommon claim is that is safe e.g. to publish (personal) data on those platforms, as it would just resemble sharing information with friendo as it used to be face-to face.»,* en página 2.

[46] Véase el Monográfico: «V Congreso Internet, Derecho y Política (IDP) Cara y cruz de las redes sociales» en la *Revista de Internet, Derecho y Política*. Universidad UOC. Núm. 9, Diciembre 2009.

[47] En la Directiva y la ley española se define «**dato personal**»: «Cualquier información concerniente a personas físicas que permita su identificación directa o indirectamente». La Comisión europea, y en colaboración con las Agencias de Protección de datos, está trabajando en un nuevo concepto más amplio. Véase: «Contribución de la Agencia Española de Datos a la Consulta de la Comisión sobre un enfoque global de la protección de datos personales en la Unión Europea» Madrid, 2011. Disponible en www.aqpd.es

[48] **Fichero**: «Todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso».

[49] «Interés general» e «interés publico general», véase el trabajo citado de Guichot, E., Transparencia y acceso…, oc.

[50] La Ley define así el «**tratamiento de datos**»: «Operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias».

su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado». Ahora bien, siempre que una Ley no disponga lo contrario, el afectado podrá oponerse al tratamiento en los términos del artículo 6.4. El artículo 6, (excepciones al consentimiento, y sin olvidar los arts.7.2 y 8 sobre datos sensibles) en relación con el 11, apartados 2 y 6 (excepciones a la comunicación de datos) y los artículos 27, 28 y 29, referidos a las fuentes de acceso público, **resumen las razones de interés público general que pueden primar sobre los datos personales contenidos en ficheros privados**[51]**. Razones de Estado**[52]**, o razones económicas, científicas, históricas o informativas, básicamente.**

2.1.1. El perfil del usuario

Si acotamos el concepto de red social online como «**servicios prestados a través de Internet que permiten a los usuarios generar un perfil, desde el que hacer públicos datos e información personal y que proporcionan herramientas que permiten interactuar con otros usuarios y localizarlos en función de las características de los perfiles**»[53], no cabe duda que hay que partir de ese elemento imprescindible de la red social que es el perfil del usuario[54], donde parece concentrarse casi todos los riesgos para la protección de datos y la privacidad. Establecidas las **condiciones de uso y políticas de pri-**

[51] Véase más arriba la nota núm.38 donde se recogen las excepciones de cada tipo de ficheros o las que afectan a ambos, privados o públicos.

[52] La Recomendación del CONSEJO DE MINISTROS EUROPEOS, ya citada más arriba, CM/Rec(2010)13, sobre la protección de datos personales automatizados para la creación de perfiles, en su artículo 6 establece las excepciones y restricciones a los derechos del individuo cuando: «*where it is necessary in a democratic society for reasons of state security, public safety, the monetary interests of the state or the prevention and supresión of criminal offences, or protecting the data subject or the rights and freedoms of the others, member states need not apply the provisions set out in Section 3,4and 5 of the present recommendation, where this is provided for in law*».

[53] Estudio sobre la privacidad de los datos y la seguridad de la información en las redes sociales online., o.c., disponible en: www.agpd.es

[54] En la Recomendación CM/Rec (2010) 13, arriba citada, se define «perfil», aunque en un contexto más amplio que el usado en las redes sociales, pues la Recomendación se refiere a la creación de perfiles en Internet a partir de todos los datos visibles e invisibles de los usuarios, como: «*Profile: refers to a set of data characterising a category of individuals that is entended to be applied to an individual*». E inmediatamente después: «*Profiling: means an automatic data proccessing techinique that consists of applying a profiles to an individual,particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferentes, behaviours and attitudes*».

vacidad en el SRS (sitio de la red social), por parte del prestador del servicio, el usuario al registrarse, presumiblemente conociendo y asumiendo tales condiciones de privacidad y seguridad, va a proporcionar voluntariamente información personal necesaria para poder operar en la red social. Y se le van a requerir datos en el formulario de registro que, aunque quizá no obligatorios, pueden ser excesivos, sin una definición concreta o determinada de su finalidad; y sujetos normalmente a la transferencia internacional de datos, pues la mayoría de los servidores y establecimientos de estas plataformas radican en USA; e incluso el grado de publicidad del perfil puede ser por defecto[55] muy elevado. Estos y otros riesgos que se pueden detectar en cada registro de cada SRS son, ciertamente, graves. **Pero, cabe añadir que, el sujeto es consciente cuando lo realiza, y tan consciente y libre ha de ser una voluntad para firmar un acuerdo o contrato en el mundo real como en el virtual. Es un ejercicio de libertad, que salvo en el caso de los menores, queda a meced de los ciudadanos.** De ahí la importancia de que las políticas de privacidad y condiciones de uso deban ser claras e inteligibles, desde un primer momento, para que el **consentimiento informado**[56] del usuario sea tal. Pues va a **aportar voluntariamente un conjunto de datos personales** que pueden comprometer no sólo su privacidad sino otros derechos fundamentales también. **Sin embargo, el perfil es sólo la punta del iceberg, pues los verdaderos riesgos se ocultan en** las aplicaciones de programas del servicio y en otros mecanismos de software, que captan los usos, comunicaciones e interacciones del usurario **sin advertirle.** En el registro del perfil, normalmente, el usuario decide lo que hace público, semipúblico o privado, dentro de un sistema delimitado, y ejerce, de alguna manera, esa «autodeterminación informativa»[57]. **Es pues una falacia centrar la atención sólo en el formulario del perfil en orden a proteger los datos personales y la privacidad.**

Además de este perfil, en la mayoría de estos sitios, con una u otra fórmula, se añaden **listas de contactos de familiares, amigos, conocidos y desconocidos**

[55] Puede resultar el perfil de acceso completamente público, lo que supone un grave riesgo para la seguridad de los datos personales del usuario, pues serán accesibles por parte de cualquier usuario de la plataforma.

[56] El principio de consentimiento y el de finalidad son pilares básicos en la protección de datos personales. Art. 7 LOPD.: Este artículo obliga a contar con un consentimiento expreso y por escrito en lo que se refiere a datos relativos a ideología, religión o creencias, y expreso en el ámbito de la salud, origen racial y vida sexual.

[57] Expresión que tiene su origen en la jurisprudencia del Tribunal Constitucional Alemán, y que en España recoge y acuña: LUCAS MURILLO, P. (1990). *El derecho a la autodeterminación informativa.,* Tecnos, Madrid, 1990.

o de profesionales, compañeros de trabajo o no. Danah Boyd[58] define «Facebook» como «un sitio de redes sociales en el sentido de que es un servicio basado en la red que permite a los individuos (1) crear un perfil público o semipúblico dentro de un sistema delimitado, (2) articular una lista de otros usuarios con los que tienen conexión y (3) visualizar y entrecruzar su lista de conexiones y las realizadas por otros dentro del sistema». Aunque referido a esa red social en concreto, cierto es que, en términos generales, es extensible a otros sitios[59], y el caso de estudio de *Facebook* puede ser paradigmático, *mutatis mutandis,* para comprender y analizar muchas de estas redes, sin perjuicio de ir al caso concreto, para cada una de ellas, en cuestiones legales puntuales. «Adicionalmente, la característica principal de un sitio como *Facebook* es conectar los perfiles de los participantes con sus identidades públicas, usando nombres reales y otros modos de identificación del mundo real, como fotografías, vídeos o direcciones de correo electrónico, permitiendo así la interacción y comunicación entre individuos del mundo real. Por tanto, *Facebook* está muy lejos de equiparse a los espacios de chat con pseudónimo y no se puede considerar únicamente como un patio de recreo para "entes virtuales" en el que las identidades son flexibles y están desconectadas de sus "cuerpos reales". De hecho, no hay casi nada virtual en lugares como *Facebook*»[60]. De ésta manera, y en principio, cabe esperar que cada usuario «diseñe» el nivel de publicidad de su perfil, su lista de contactos los cuales tienen acceso al mismo y con los que interactúa, y si además otros, como el resto de los usuarios o los amigos de sus

[58] BOYD, D., ELLISON, N., «Social Network Sites: Definition, History, and Scholarship» en *Journal of Computer-Mediated Communication,* Vol.1, núm.13. Disponible en: http://jcmc.indiana.edu/vo13/issued1/boyd.ellison.htm

[59] Así, por ejemplo, en *Facebook* los «contactos» se denominan «amigos» y se necesita su aprobación para incluirlos en tu lista. Mientras que en *Twiter* los contactos son tus «seguidores», y no se necesita comunicárselo o su autorización. En *Lindken* los contactos se asumen profesionales, se necesita su aceptación a ser incluidos en tu lista, y se crean grupos de diferente carácter con los que te relacionas. Estas y otras diferencias también se traducen en diferencias técnicas en las aplicaciones de estas redes, tal como en los interfaces. Y también de ello se derivan consecuencias de diverso orden, psicológico, social y jurídico. La confianza que genera el término amigo puede llevar a un uso no correcto de la información proporcionada. Pues entre los amigos pueden ser incluidos perfectos desconocidos o simplemente conocidos, profesionales colegas o compañeros de trabajo, familiares o, incluso, amigos.

[60] DUMORTIER FRANCK. (2009). «Facebook y los riesgos de la "descontextualización" de la información», en *Revista de Internet, Derecho y Política.* Revista de los Estudios de Derecho y Ciencia Política de la UOC. Núm. 9. Diciembre de 2009. p. 27. También véase: GRIMMELMANN, J. (2009) «Saving Facebook». *Iowa Law Review.* Vol. 94, págs. 1137-1206. Téngase en cuenta que, tanto DUMORTIER como GRIMMELMANN, consideran en sus trabajos las aportaciones de SOLOVE. Véase: SOLOVE, D.J., (2007), *The future of reputation. Gossip, rumor, and privacy on the internet,* New Heaven and London, Yale University Press. Especialmente el capítulo septimo, p. 161.

amigos, hasta donde decida, acceden o no al mismo. En definitiva, desde lo más privado que aparentemente le ofrece la plataforma, pasando por estadios semipúblicos o semiprivados, hasta perfiles y espacios totalmente públicos. Aunque, como mínimo, algunos datos siempre van a ser públicos, como su nombre o la lista de contactos necesarios para que opere el cruce de relaciones que el proveedor de servicio le facilitará o que él mismo decida realizar.

Se puede producir un gran arco de posibilidades en cuanto al número de contactos de cada usuario y el cruce con otros, la naturaleza de la relación o interacción que mantenga con ellos y el acceso permitido que tengan a su espacio e información: Desde contactos estrictamente personales, confidenciales, privados y muy reducidos, pasando por contactos de amigos, familiares o profesionales de forma más o menos abierta hasta contactos de todo tipo, incluidos los desconocidos, con los que puede conectar de forma totalmente pública o privada. Puede ocurrir que un perfil muy estricto que sólo permite el acceso a sus familiares y amigos íntimos, por ejemplo, pueda constituir una lista de de hasta cien contactos, por lo menos[61]. Así, ¿Puede considerarse privado? ¿se aplicaría la exención doméstica en el tratamiento de datos?. Toda red social —en general, aunque en las virtuales se están detectando las diferencias— se fundamenta en la *teoría de los seis grados de separación*, en virtud de la cual cualquier individuo puede estar conectado a cualquier otra persona en el planeta, a través de una cadena de conocidos con no más de cinco intermediarios (con un total de seis conexiones). La cifra de conocidos aumenta a medida que lo hacen los eslabones de la cadena. Los individuos de primer grado serán los más próximos y según se avanza en el grado de separación, disminuye la relación y la confianza.[62] El riesgo de lo que se ha llamado la «descontextualización de la información» amenaza en las redes virtuales conforme los contactos son de diferentes y distanciados eslabones, y más allá de la protección de datos, **el concepto convencional de privacidad**[63] que-

[61] Y aunque el primero no permita que los «amigos de sus amigos» accedan y compartan su información, nada obsta para que hasta sus más íntimos puedan hablar de ello o compartirlo con otros contactos de la misma red.

[62] En el estudio de INTECO y la AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, ya citado, se recoge a pie de página la fuente de tal teoría: Teoría inicialmente propuesta en 1929 por el escritor húngaro FRIGYES KARINTHY. Recogida también en el libro «Six degrees: The Science of a Connected Age» del sociólogo DUCAN WATTS, quien asegura que es posible acceder a cualquier persona del planeta en tan solo seis «saltos», p. 34.

[63] DUMOTIER, FRANCK., oc. «En esta perspectiva, el derecho a la privacidad se puede concebir como un «derecho a la autodeterminación del yo contextual que le garantiza la posibilidad de actuar y comunicarse como desee contextualmente sin tener que temer una descontextualización inadecuada de sus comportamientos o de la información», p. 35. Sobre el concepto convencional de privacidad e intimidad: HERRERO TEJEDOR,F. (1998) *La intimidad como derecho fundamental.,* Madrid, Colex.

da también desdibujado. Pues significa que la persona define el ámbito de la misma en cada contexto y tiempo de su vida, personal, profesional o social[64], siendo, aún así, siempre ella misma. «Mientras que el derecho a la privacidad garantiza al ser humano la posibilidad de contar con muchas facetas y actuar de forma contextualmente diferente a fin de asegurar la perseverancia de una democracia vívida y que permita el debate», el derecho a la protección de datos «es una herramienta para dotar a los "dividuos contextuales" de medios para asegurar la integridad contextual de su imagen informativa»[65], pero, por contraste, el importante **principio de finalidad, esencial en la legislación de datos,** se presenta muy comprometido en estas redes, al igual que el de **adecuación**[66], pues en las condiciones de uso y privacidad la finalidad aparece indefinida o tan ampliamente concebida que es impredecible. «El mismo artículo de la Directiva (art. 4)[67] también requiere que los datos sean adecuados, relevantes y no excesivos con relación al fin para el que se obtienen y/o procesan, exigiendo que la obtención y difusión de la información sean adecuados para ese contexto y obedezcan las normas de información aplicables en él».[68] Y como afirma el mismo autor «de hecho, la multi-contextualidad global no se puede cubrir con un derecho a la protección de datos porque, cuando la finalidad de un servicio se define como "todo", todos los datos se pueden considerar adecuados, relevantes y no excesivos y cualquier distribución ulterior se puede considerar compatible[69]. Además, para dimensionar lo anterior, es útil recordar que tanto en la Directiva en su artículo 7.b) y c), como en la LOPD en su artículo 6.2, el consentimiento del interesado no se exige cuando «es necesario (el tratamiento) para la ejecución de un contrato en el que el interesado sea parte o para la aplicación de medidas precontractuales adoptadas a petición del interesado» (Directiva, 7.b) o 7.c) «es ne-

[64] DUMOTIER, F., «Facebook y los riesgos de la "descontextualización" de la información», o.c.,: «De estas observaciones se deriva una amenaza de descontextualización: la dificultad que tiene un ente con múltiples facetas para restringir la información que desea compartir con «amigos» de distintos contextos» p. 29 «El riesgo de descontextualización no sólo supone una amenaza para el derecho a la protección de datos, es decir, el derecho a controlar la identidad informativa que un ser humano proyecta en un cierto contexto. De un modo más fundamental, es una amenaza al derecho de privacidad como ser humano: el derecho del ser humano a ser un yo múltiple y gregario sin una discriminación injustificada», p. 36.

[65] DUMOTIER, FRANCK., oc., p. 38.

[66] Ibid., p. 38 «En otras palabras, la finalidad descrita en la página principal de Facebook —"Facebook te ayuda a comunicarte y compartir tu vida con las personas que conoces"— es excesivamente amplia como para determinar qué datos son adecuados, relevantes y no excesivos con relación a dicha finalidad».

[67] Directiva 95/45/CE.

[68] Ibid., p. 38.

[69] Ibid., p. 38.

cesario para el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento". En términos parecidos la Ley española, art. 6.2 «...cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento...».

De manera que, teniendo en cuenta las condiciones de la relación jurídica contractual que se establece entre el prestador del servicio y el usuario, las posibilidades de tratamiento y sus fines pueden ser muchas y muy variadas en la más completa legalidad (conforme la Directiva y la Ley). **Hay que cuestionarse si la protección de datos personales es una herramienta jurídica adecuada para asegurar la privacidad de las personas en la red.** Autores como Lessig[70] propugnan soluciones conjuntas donde converjan legislación, software e intereses personales de empresas y consumidores, pues en Internet gran parte de la cuestión reside sobre «privacy in public».

Y volvemos a reflexionar de nuevo sobre la misma pregunta: un perfil de escasos datos públicos, con una lista muy reducida de contactos de familiares y/o amigos, por ejemplo, pero con los que comparte información e incluso éstos con los «amigos de sus amigos» (y estos a la vez cruzan contactos e informaciones) que pudieran bien ser medios de comunicación de diferentes partes del mundo o cualquier tipo de institución pública, por ejemplo. ¿Puede aplicarse la exención doméstica? ¿Estaríamos ante comunicación privada y confidencial? **¿Quién define, en definitiva, lo público y lo privado? La persona, la plataforma, el número de contactos y sus derivaciones, la naturaleza de la relación, el grado de parentesco o la finalidad del tratamiento de los datos. Ocurre, sin embargo, que todo esto se mezcla e intercambia y superpone en una misma cuenta y espacio de usuario a la vez.** «Cuando el acceso al perfil de información va más allá de los contactos seleccionados por el usuario, por ejemplo a todos los usuarios de la red social, o cuando el usuario debe aceptar contactos, independientemente de la relación que tengan con él, o si el dato no se puede indexar mediante un motor de búsqueda, nos encontraríamos con un acceso equivalente a público. Esto podría suponer la aplicación al usuario de la Directiva de protección de datos, por la que le asimilaría a las responsabilidades que adquiere un responsable de una base de datos. Puesto que no se trataría ya de un ámbito doméstico, sino público... En esta línea, puesto que no concurre la excepción de uso doméstico, sería necesario proteger los derechos de terceros, sobre todo con re-

[70] LESSIG, LAWRENCE., (2006), *Code versión 2.0,* N.Y, Basic Book. Perseus Books Group, p. 200, y en la página 230 donde afirma «It is Law helping Code to perfect privacy Policy».

lación a sus datos sensibles»[71]. Esta es una de las conclusiones a las que ha llegado la doctrina científica, que aunque parcialmente aquí se comparte, también podría objetarse que el usuario, en ese caso, actúa amparado por las excepciones de libertad de expresión o de creación.

El usuario podría ser considerado como responsable de tratamiento de datos, en su caso[72], además del prestador del servicio respecto al fichero privado que constituyen todos los registros de perfiles y contactos, e independientemente de la responsabilidad sobre los datos de tráfico, localización y conservación del proveedor de servicios de comunicación en Internet. La vocación de fuente de información pública parece estar en la esencia de estos sitios de colaboración, aunque puedan encajar en la definición legal de ficheros privados. **Exención de ámbito doméstico en el tratamiento de datos, ficheros privados y fuentes accesibles al público, son categorías que están implicadas en el complejo entramado de contactos, datos, informaciones e interacciones que son las redes sociales online.**

2.1.2. Las comunicaciones e informaciones de los usuarios y miembros

Una vez instalado el usuario en el sitio de la red social online, va a desarrollar una actividad en la plataforma utilizando los servicios y herramientas que ésta le ofrece. Bien puede comunicarse y escribir mensajes o subir fotos e imágenes o cualquier otro tipo de material (películas, música, etc.,) en el llamado «muro» o pared, lo que queda expuesto a todos sus contactos con acceso; bien puede comunicarse mediante e-mail, de una manera absolutamente secreta y confidencial con la persona/s que desee; bien puede realizar un link a un *blog* personal o de otras personas, a páginas *webs,* personales o de otro tipo, a redes privadas, etc.; bien puede escribir en la pared de sus contactos y ellos en la suya, e intercambiar todo tipo de informaciones y expresiones. En definitiva, puede publicarse exce-

[71] ROIG, ANTONIO. (2009). «E-privacidad y redes sociales» en *Revista de Internet, Derecho y Política*. Núm. 9 Diciembre, 2009, p. 46.

[72] Si no se aplica la exención de «ámbito doméstico», por tratarse de actividades que lo trascienden. Véanse, por todas, las Sentencias del TJUE *Lindqvis*t y *Satamedia*. En la primera, sobre la exención domestica, y en la segunda, sobre la excepción de la libertad de información:- STJUE de 6 de Noviembre 2003. En el asunto C-101/01, que tiene por objeto una petición dirigida al TJ, con arreglo al art.234 CE, por el *Göta hovrätt* (Suecia), destinada a obtener, en el proceso penal seguido ante dicho órgano jurisdiccional contra *Bodil Lindqvist*, una decisión prejudicial.

— STJUE de 16 de Diciembre 2008. En el asunto C-73/07. *Tietosuojavaltuutettu* contra *Satakunnan Markkinapörssi Oy y Satamedia*. Asunto que tiene por objeto una petición prejudicial planteada, con arreglo al art.234 CE, por el *Kortein hallinto-oikeus* (Finlandia).

siva información propia o de terceros, que no han prestado consentimiento, y de los que se está realizando una cesión[73] y tratamiento de datos. Esos terceros pueden proceder desde dentro de la red o desde fuera de la misma. Un tercero fuera de la red puede proveer datos e informaciones a través, por ejemplo, de un *blog o web,* a la cual se ha remitido por link, o acceder sin consentimiento a datos de usuarios de la red, como los desarrolladores de aplicaciones autorizados o no por el proveedor de servicio, conductas que constituyen infracción del derecho a la protección de datos o de otros derechos fundamentales.

Sin intención de agotar la relación de riesgos que se pueden detectar[74] en la protección de datos personales en estas plataformas, y sólo con el fin de mostrar algunos importantes de los que constituyen la problemática, son ya muy conocidos los que proceden de la instalación y uso de «***cookies***[75]» sin conocimiento del usuario, y que pueden ser lanzadas tanto por el prestador del servicio como por otros usuarios. Igualmente, las llamadas «***web beacon***[76]», imágenes electrónicas que permiten al sitio conocer quién y qué contenido online ha sido visitado. Normalmente estas imágenes son incluidas en correos electrónicos, anuncios, etc. **De este modo, se recaban datos de forma automática e «invisible», sin conocimiento ni consentimiento del titular, al contrario que en el caso de los formularios del perfil del usuario.** Considerando que el dato de la dirección IP de un usuario en Internet es considerado dato personal[77], que puede asociarse a una persona identificable, es

[73] El Art. 3. i) de LOPD, define «cesión» o comunicación de datos: «Toda revelación de datos realizada a una persona distinta del interesado».

[74] Véase para ello el ya citado informe de ENISA: ENISA Position Paper No.1. *Security Issues and Recommendations for Online Social Networks*.

[75] Son ficheros que tienen la posibilidad de almacenar determinada información sobre el usuario y su tipo de navegación a través de un sitio web. Estos ficheros se instalan en los equipos de los usuarios, de forma que resulta posible detectar el lugar desde el que accede el usuario, el tipo de dispositivo empleado (móvil o fijo) para el acceso, el tipo de contenidos accedidos, los lugares más visitados y las acciones habituales realizadas durante la navegación, así como el tiempo empleado en cada una de las páginas, entre otras muchas funcionalidades.

[76] Una *web beacon o web bug* es una diminuta imagen en una página web o en un mensaje de correo electrónico que se diseña para controlar quién lee el mensaje. Su tamaño es inapreciable, pudiendo ser un píxel en formato GIF y transparente. Se representan como etiquetas HTML. Una *web beacon* permite tener cierta información sobre el usuario (o del visitante de una página web o del lector de mensaje de correo electrónico).

[77] Véase el informe del Grupo del Artículo 29, donde así se afirma. Aunque no se puede obviar que la cuestión no es del todo pacífica, y aún encontramos una fuerte oposición a tal consideración, pues aunque todos estos documentos tienen gran autoridad, no poseen, obviamente, fuerza legal. En el Reino Unido, recientemente, se ha dado alguna sentencia que parece no considerar la IP como dato personal, véase en *Charles Russell. IP Bulletin,* March 2011. La sentencia «Patents County Court. Media CAT Ltd v Adams and others (2011) EWPCC6, HHJ Colin Birss QC, 8.

posible obtener información mediante estas herramientas sobre los usos y hábitos en Internet de un usuario del sitio. Amén de otro tipo de datos, como el programa gestor de correo electrónico que se utiliza, sistema operativo, visualización de páginas, información de direcciones de correo electrónico válidas etc., en definitiva, son herramientas muy valiosas para la publicidad y el marketing, principalmente. Tampoco se puede olvidar, y menos minimizar, la amenaza en el derecho a la protección de datos personales que supone **la indexación automática por los buscadores o motores de búsqueda de Internet de los perfiles**[78] **de usuario.** Esto, en general, supone que los datos principales o básicos o los que capte pueden **ser accesibles públicamente en la Red de forma universal, pudiendo ser utilizados por terceros sin el control del titular de los mismos.** Asimismo, es importante la mina de datos precisos y personales que obtienen las redes sociales a través de la ***publicidad hipercontextualizada***[79]*,* que colocan al ***spam***[80] en una inocente broma, respecto a lo que ésta puede conseguir de forma automática y discreta. Y muchas son las formas de realizar el ***spam*** tanto por el usuario a favor del proveedor de la red social, a través de usos aparentemente normales, usando las herramientas y servicios de la plataforma, como a favor de un interés propio o ajeno o por otros usuarios dando entrada a terceros[81] que ven en las redes sociales efectivas formas de comunicación comercial para captar clientes e ingresos. A todo lo anterior habría que añadir otros peligros, que incluso pueden constituir delito, como la **suplantación de la identidad** del usuario en la red social (tanto de su perfil como en sus comunicaciones) o la cuestión de **la conservación**[82] **y cancelación de datos**, que tratándose de comunicaciones electrónicas tiene especial relevancia y transcendencia, y de lo que nos ocuparemos de nuevo más adelante.

De lo anterior se extrae que, **los verdaderos riegos y amenazas** en el cumplimiento de los principios de la protección de datos, y el respeto a los derechos

---

February, 2011. Disponible en: www.charlesrussell.co.uk. Aunque en sentido contrario, puede verse la Sentencia del TJE, de 29 de enero de 2008.

[78] E incluso entrar en las comunicaciones o *twitts* de los usuarios, por ejemplo en *Twitter.*

[79] Aunque evita la molesta publicidad al navegar, sin embargo, al contextualizar la publicidad conforme a los datos e informaciones personales del usuario se utilizan sus datos sin autorización. Véase: GP 29 Dictamen 2/2006 (WP118).

[80] Recepción de comunicaciones comerciales electrónicas no solicitadas.

[81] En fin son tantas las posibilidades como la imaginación de los que tienen intereses comerciales y quieren captan clientes. Aunque se verá más tarde en este trabajo, pude consultarse en el citado Estudio sobre privacidad de los datos y la seguridad de la Información en las redes sociales online. INTECO y la Agencia Española de Protección de Datos.

[82] RODOTA, S., (2006) «La Conservación de los datos de tráfico en las comunicaciones electrónicas» en *Revista de Internet, Derecho y Política,* núm. 3, pp. 53 y ss. Este trabajo gira en torno a la Directiva 2006/24/CE, sobre retención de datos en las comunicaciones electrónicas.

de los usuarios, reconocidos por ley, en este servicio de la sociedad de la información, que se sustancia mediante comunicaciones electrónicas en Internet, **tienen un rostro invisible dibujado por el software y las diferentes aplicaciones**. Es cierto que la tecnología jurídica (tecnologías PET[83]) juega un gran papel, pero no resuelve lo que parece ser la terca voluntad de estas plataformas y de los ciudadanos, que continúan día a día aumentando el número de amigos o contactos que interactúan con diversos fines en estas redes. Y, además, la problemática no deja de acrecentarse, pues la llegada de la *Web 3.0,* con los servicios de la *web* semántica, aumenta considerablemente este riesgo. Con esta nueva tecnología, los motores de búsqueda ya no se limitarán a las palabras clave sino también a sus significados, pudiendo extraer de las redes sociales mapas de significado. En consecuencia, el replanteamiento del propio concepto jurídico de «dato personal»[84] ya se está llevando a cabo. La capacidad de convertir datos inocuos, desestructurados y aparentemente sin sentido, en datos personales identificables es ya una realidad, que deja «tocado» el núcleo mismo de la legislación, que es el concepto de dato personal, alrededor del cual gira toda la normativa. Normativa que, aplicada a las redes sociales online, puede requerir cambios y nuevos conceptos jurídicos consecuentemente.

Pero la maraña de problemas no debe de ensombrecer lo que es la «grandeza» de estas redes: el ejercicio libre de la libertad de expresión e información por parte de los usuarios o ciudadanos. Tanto la Directiva 95/46/, como Directiva 2002/58 modificada por la Directiva 2009/136/CE, consideran la necesidad de conciliar los distintos derechos fundamentales con la protección de datos personales, y el artículo 9 de la Directiva 95 establece: «Tratamiento de datos personales y libertad de expresión: En lo referente al tratamiento de datos personales

[83] *Privacy enhancing technologies* o tecnologías garantes de la privacidad. Entre ellas, pueden distinguirse: La P2DM (*privacy-preserving data mining*), o protección tecnológica contra los motores de búsqueda o minería de datos; la protección tecnológica del acceso, de la identificación y de los sistemas de reputación; sistemas de reputación garantes de la privacidad no basados en el acceso; o la TET (*transparency enhancing technologies*), la tecnología para la transparencia, el contexto y la finalidad. Un trabajo que explica y pone en contexto estas tecnologías en: ROIG ANTONIO. (2009). «E-privacidad y redes sociales», en la *Revista IDP, Revista de Internet, Derecho y Política*., núm. 9, pp. 47 y ss.

[84] Véanse entre otros: La Contribución de la Agencia Española de Protección de Datos a la Consulta de la Comisión (europea) sobre un enfoque global de l protección de datos personales en la Unión Europea, o.c.; también, del Grupo del artículo 29, El Dictamen 4/2007, sobre el concepto de datos personales. En el mismo se afirma «la identificación a través del nombre y apellidos es en la práctica la más habitual, esa información puede no ser necesaria en todos los casos para identificar a una persona. Así puede suceder cuando se utiliza "identificadores" para singularizar a alguien».

con fines exclusivamente periodísticos o de expresión artística o literaria, los Estados miembros establecerán, respecto de las disposiciones del presente capítulo, del capítulo IV, exenciones y excepciones sólo en la medida en que resulten necesarias para conciliar el derecho a la intimidad con las normas que rigen la libertad de expresión». Y en la Directiva 2009/136/CE, artículo 2.2. 1).1., se lee: «La presente Directiva establece la armonización de las disposiciones nacionales necesaria para garantizar un nivel equivalente de protección de las libertades y derechos fundamentales y, en particular, del derecho a la intimidad y la confidencialidad, en lo que respecta el tratamiento de los datos personales en el sector de las comunicaciones electrónicas, así como la libre circulación de tales datos y de los equipos y servicios de comunicaciones electrónicas en la Comunidad». Se ha de encontrar la clave jurídica para que lo que *Yochai Benkler*[85] ha llamado «**la riqueza de las redes**» rinda sus mejores frutos a la sociedad, y que sólo por el **principio de proporcionalidad se mida la posible restricción de derechos individuales a favor de intereses generales sociales.**

En efecto, el uso de las redes tanto por personas físicas privadas o públicas, personas jurídicas, empresas, organizaciones o instituciones de todo tipo, e incluso por los propios medios de comunicación**, transforman a estas «plataformas colaborativas» en fuentes de información y, a su vez, en fuente de**

[85] BENKLER YOCHAI. (2006). *The Wealth of Networks. How Social Production Transforms Markets and Freedom*, Yale University Press, USA, 2006. El autor fundamenta desde un análisis económico-político y jurídico las relaciones sociales que las nuevas tecnologías de la información han dado lugar, provocando, más allá de la anécdota, importantes cambios: La producción industrial de la información está siendo desplazada por la producción social de la información, que los mismos individuos aportan. Las nuevas tecnologías van cambiando la producción y distribución de la información. Cambian también las estructuras, y en consecuencia se da un cambio en la información, el conocimiento y la cultura. La vieja concepción liberal económica de producción de información está amenazada, y a la vez amenaza las nuevas formas emergentes. Ya no se requieren materiales costosos para la producción de la información, que antes estaba en manos de unos pocos, centralizada. La nueva economía de la información se caracteriza por la descentralización, nuevas tecnologías y herramientas de producción a bajo precio, accesibles para todos. No se requieren materiales o herramientas costosas para la producción de la información, que estaba en manos de unos pocos. Al removerse las constricciones materiales/físicas/, se ha hecho que la creatividad y la nueva economía de la información san el corazón estructurante de la «nueva economía» de la información informatizada De tal manera que cada individuo puede crear y producir información solo o unido a otros, con un impacto o extensión mundial, sin necesidad de la organización convencional del mercado. Todo ello no sólo tendrá un impacto en las economías industriales sino también en las democracias liberales contemporáneas. Dice textualmente el autor «*Looking at the aggregate effect, we see that at all these layers (physical, logical and content layers) a series of battles is being fought over the degree to which some minimal set of basic resources and capabilities necessary to use and participate in constructing the information environment will be available for use on a nonproprietary, nonmarket basis»,* p. 392

fuentes de información[86]. La defensa del derecho a la protección de datos personales, como del resto de los derechos fundamentales en estas redes sociales online, es indiscutiblemente necesaria. Ahora bien, desde el momento que éstas **no sólo constituyen bases o ficheros de datos, sino que son «algo más», donde el derecho a la información y el derecho a la libertad de creación** se ejercen y despliegan sin precedentes por los ciudadanos, —y en cuyo ejercicio, obviamente, también la cuestión de protección de datos se ve involucrada—, **es necesario plantease si se deben contemplar desde otra perspectiva jurídica. Perspectiva que permita armonizar el derecho a la protección de datos personales con las libertades de creación e información y expresión.**

2.2. Las redes sociales como posibles fuentes de acceso público

Se ha indicado más arriba, que una de las principales excepciones al consentimiento, que permite sin éste tratar datos personales en el sector privado, es lo que el artículo.3, apartado J) de la LOPD, define como **fuentes accesibles al público**: «aquellos ficheros cuya consulta puede ser realizada, por cualquier persona, no impedida por una norma limitativa o sin más exigencia que, en su caso, el abono de una contraprestación» Y seguidamente enumera las fuentes de acceso público que exclusivamente tienen esa consideración, y que son esas y sólo ésas: —el censo promocional, —los repertorios telefónicos en los términos previstos por su normativa específica, —las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de: a)nombre b)título c)profesión d) actividad e) grado académico f) dirección g) indicación de su pertenencia a un grupo, —los diarios y boletines oficiales, —y los medios de comunicación.

El artículo 28 de la misma Ley establece su regulación en el contexto del sector privado y dice: «1. Los datos personales que figuren en el censo promocional,

[86] Me refiero a que los usuarios pueden ahí suministrar información de todo tipo, por ejemplo, la información en vivo y simultánea de los acontecimientos de las recientes «revoluciones de países árabes», que ni siquiera los medios de comunicación son capaces de dar tan rápidamente y desde tantas fuentes. El medio de comunicación, fuente de información, acude a la fuente viva de las redes. Y a su vez, estos medios tienen presencia como usuarios en muchas de estas redes (*twitter, facebook*.). La Empresas tienen presencia en las redes como usuarios que se relacionan con los otros usuarios como manera de hacer clientes y negocio. Ya se ha acuñado el término de «*community manager*» asignado a los profesionales que en las empresas u organizaciones gestionan las redes en las estrategias de negocio. De todo ello, se habló en el Congreso de Redes Sociales, que tuvo lugar en Burgos, el pasado mes de febrero de 2011.

los repertorios telefónicos o las listas de personas pertenecientes a grupos profesionales a que se refiere el artículo 3.j) de esta Ley deberán limitarse a los que sean estrictamente necesarios para cumplir la finalidad a que se destina cada listado. La inclusión de datos adicionales por las entidades responsables del mantenimiento de dichas fuentes requerirá el consentimiento del interesado, que podrá ser revocado en cualquier momento. 2. Los interesados tendrán derecho a que la entidad responsable del mantenimiento de los repertorios de abonados al servicio telefónico y de los Colegios profesionales indique gratuitamente que sus datos personales no pueden utilizarse para fines de publicidad o prospección comercial. Los interesados tendrán derecho a exigir gratuitamente la exclusión de la totalidad de sus datos personales que consten en los repertorios telefónicos y en el censo promocional por las entidades encargadas del mantenimiento de dichas fuentes. La atención a la solicitud de exclusión de la información innecesaria o de inclusión de la objeción al uso de los datos para fines de publicidad o venta a distancia deberá realizarse en el plazo de diez días respecto de las informaciones que se realicen mediante consulta o comunicación telemática y en la siguiente edición del listado cualquiera que sea el soporte en que se edite. 3. Las fuentes de acceso público que se editen en forma de libro o algún otro soporte físico perderán el carácter de fuente accesible con la nueva edición que se publique. En el caso de que se obtenga telemáticamente una copia de la lista en formato electrónico, esta perderá el carácter de fuente de acceso público en el plazo de un año, contando desde el momento de la obtención originaria». Y los siguientes artículos regulan algunas fuentes concretas. El cumplimiento del principio de calidad de los datos se pretende con el plazo establecido para utilizar los datos incluidos en una fuente de acceso público, momento a partir del cual, si se quieren seguir utilizado los datos, será necesario el consentimiento del interesado. La diferenciación entre soporte físico y soporte electrónico es relevante a efectos de plazos y el ejercicio de los principios y derechos.

En el sector público, en el artículo 21.3 se lee: «Cesión de datos entre Administraciones Públicas. 3. No obstante lo establecido en el artículo 11.2.b), la cesión de datos recogidos de fuentes accesibles al público no podrá efectuarse a ficheros de titularidad privada, sino con el consentimiento del interesado o cuando una Ley prevea otra cosa» (el artículo 11.2.b. excluye la necesidad de recabar el consentimiento del interesado cuando lo datos son recogidas de fuentes de acceso público). Asimismo, el artículo 11 de la Directiva 95/46/CE, dice: Información cuando los datos no han sido recabados del propio interesado: 1. Cuando los datos no hayan sido recabados del interesado, los Estados miembros dispondrán que el responsable del tratamiento o su representante deberán, desde el momento del registro de los datos, o, en caso en que se piense comunicar datos a un

tercero, a más tardar, en el momento de la primera comunicación de datos, comunicar al interesado por lo menos la información que se enumera a continuación, salvo que el interesado ya hubiera sido informado:…».

Es cierto que en la enumeración tasada de la Ley española en el artículo 3.j) no se incluye, ni enumera, expresamente a Internet ni cualquier herramienta o recurso de Internet. Obviamente, la Ley española es una implementación de la Directiva 95/46/CE, cuyo ámbito no incluye al sector de las comunicaciones electrónicas, aunque las Directivas 58/2002/CE, y su modificación por la Directiva 136/2009/CE, a ella se remiten, para las disposiciones generales o para resolver aquellos aspectos de la protección de datos y privacidad que ellas no regulen especialmente en el sector de las comunicaciones electrónicas. Es por ello que, para la específica fuente de acceso público que son los «repertorios telefónicos», haya que acudir a estas Directivas y a la legislación sectorial específica que implementan estas Directivas[87]. La Agencia de Protección de datos ha sido tajante a este respecto en distintas resoluciones, y ha afirmado que «de la lectura del tenor literal del citado precepto —3.j— no se desprende que las páginas *web* puedan ser consideradas como fuentes accesibles al público a efectos de la LOPD. Podría argumentarse que la citada enumeración no es taxativa, por cuanto, con carácter previo a la misma, el 3.j) indica que son fuentes accesibles al público «aquellos ficheros cuya consulta puede ser realizada por cualquier persona, no impedida por una norma limitativa, o sin más exigencia que, en su caso, el abono de una contraprestación». Sin embargo, ello en modo alguno impide que resulte de aplicación una interpretación que propugne una enumeración taxativa, dado que el contenido de este primer inciso indica un requisito indispensable para que los ficheros enumerados por la propia norma puedan ser considerados como fuentes de acceso público… En consecuencia, la utilización de los datos de carácter personal que figuran en páginas *web* por persona o entidad distinta a los interesados, en cualquier caso necesitaría para su tratamiento el consentimiento previo de los mismos, no pudiendo considerarse fuente de acceso público[88]».

[87] Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones. Y el Real Decreto 424/2005 de 15 de Abril, que establece las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios. El Reglamento aborda la protección de los datos de carácter personal desde un triple prisma: los datos de tráfico, facturación y localización; la prestación de servicios avanzados de telefonía y la elaboración de las guías telefónicas de números de abonados.

[88] Resolución/00574/2005 de la AEPD. Razonamiento que ha mantenido en la resolución de otras consultas similares.

Nadie duda de la autoridad y competencia de la Agencia (AEPD), en la interpretación y aplicación de la Ley, con anterioridad a la vía jurisdiccional; sin embargo, es lícito criticar sus resoluciones, como lo es hacerlo de las sentencias judiciales. Parece lógico que la Agencia se mantenga fiel a su fin y que, mientras que la Ley no cambie o se modifique, se mantenga lo más fiel posible a la misma. Y parece lógica también su interpretación rígida y formalista. Sin embargo, la Directiva 45/96, al no adoptar la siempre arriesgada técnica de enumeración, —y no enumera las fuentes públicas y formula las excepciones en términos amplios como lo hace en el reproducido arriba artículo 11 (entre otros)—, permite adaptar la Directiva, de alguna manera, a la evolución tecnológica y de la sociedad. Es cierto que las Directivas de comunicaciones electrónicas o la de la Sociedad de la Información tampoco dicen nada concreto, y remiten a las disposiciones generales de la Directiva 95/46/CE. Las citadas Directivas del 2002 y 2009, sin embargo, sí regulan las concretas y especiales cuestiones de las guías telefónicas y del *spam*, que sí se aplicarían a los servicios de las redes sociales, como se verá. **La evolución de Internet y sus usos** (que no estaban en la mente del legislador comunitario o español), en concreto estos servicios de la sociedad de la información que son las redes sociales online, así como todas las problemáticas que provocan, y algunas se han señalado, **nos permiten, con legitimidad, proponer una interpretación diferente o, todavía más, una modificación o legislación diferente.** La importancia social, económica y política de Internet es ya incuestionable e imparable y, concretamente, la de estas redes sociales online, y negarlo es ignorar la realidad.

Es por ello que no sea descabellado pensar en estas redes como fuentes de información de acceso público de naturaleza mixta o híbrida, atendiendo a la vigente legislación: por una parte, se asimilarían a los repertorios telefónicos y guías profesionales *mutatis mutandis*, y por otra, a los medios de comunicación. Obviamente, sería necesario actualizar el contenido, los límites y garantías a favor de los usuarios en un medio técnico tan complejo, en aras al equilibrio necesario entre derecho a la información y derecho de protección de datos personales. Como se reconoce en el Dictamen 5/2009, del G29, «debe tenerse en cuenta que, aunque la exención doméstica no se aplique, el usuario SRS puede beneficiarse de otras exenciones, como la exención con fines periodísticos, artísticos o literarios. En estos casos, debe establecerse un equilibrio entre la libertad de expresión y el derecho a la intimidad».[89] Son, en base a estos

[89] O.c., p. 7.

y otros fines o exenciones, las razones que pueden fundamentar que estos sitios son fuentes de información de acceso público.

2.3. Alcance del uso de los datos de las redes sociales online como fuentes públicas

Pensar en fuentes de datos accesibles al público no significa disponer de «un cheque en blanco» para acceder a los mismos y utilizarlos o tratarlos libremente según nuestros intereses. Así en la legislación vigente se encuentra: que conforme al artículo 11.2.b) no es necesario recabar el consentimiento del titular del dato incluido en una fuente pública para su cesión a un tercero, aunque sí si la transferencia se realiza por la Administración a un fichero privado (art.21.3); y observando el plazo de vigencia como fuente pública señalado en la Ley, con el fin de cumplir con el principio de calidad de los datos. Asimismo, hay que tener presente lo que dispone en la misma Ley el artículo 6.4 «en los casos en los que no sea necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal, y siempre que una ley no disponga lo contrario, éste podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En tal supuesto, el responsable del fichero excluirá del tratamiento los datos relativos al afectado». Y conforme al arriba citado artículo 28, el interesado tiene derecho a la exclusión o a que no se añadan datos adicionales que no estén previstos o a que sólo figuren los necesarios para cumplir con la finalidad de lo que constituye la fuente de información pública. Pero aún más, y como premisa de partida aplicable a todas las bases o ficheros, incluidos los que contienen fuentes públicas, la Ley orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, permite a los afectados por un tratamiento de datos el ejercicio de los derechos de rectificación, cancelación y oposición. Y cuando los datos de fuentes de acceso público, se traten con fines de publicidad y de prospección comercial, «de conformidad con lo establecido en el párrafo segundo del artículo 5.5.de esta Ley en cada comunicación que se dirija al interesado se informará del origen de los datos y de la identidad del responsable del tratamiento, así como los derechos que le asisten» (art.30). Y la Ley, como premisa, igualmente vincula a todos los responsables de ficheros al cumplimiento de los principios que la misma consagra: finalidad, actualización, exactitud y calidad o conservación.

No hay que olvidar la famosa STC 292/2000 del Tribunal Constitucional, que pone de relieve la capacidad reactiva del titular de los derechos, cuando sienta «el derecho a la protección de datos atribuye a su titular un haz de facultades consistentes en diversos poderes jurídicos cuyo ejercicio impone a ter-

© UNED. *Revista de Derecho Político*
N.º 81, mayo-agosto 2011, págs. 101-154

ceros deberes jurídicos, que no se contienen en el derecho fundamental a la intimidad, y que sirven a la capital función que desempeña este derecho fundamental: garantizar a la persona un poder de control sobre sus datos personales, lo que sólo es posible y efectivo imponiendo a terceros los mencionados deberes de hacer. A saber: el derecho a que se requiera el previo consentimiento para la recogida y uso de los datos personales, el derecho a saber y ser informado sobre el destino y uso de esos datos y el derecho a acceder, rectificar y cancelar dichos datos. En definitiva, el poder de disposición sobre los datos personales (STC 254/1993, FJ/)».

Que los datos figuren en fuentes accesibles al público significa que existe alguna excepción a los derechos y principios de la persona, excepciones tasadas y delimitadas por Ley, pero nada más: el sujeto mantiene su poder de control y disposición sobre sus datos. Como bien ha entendido el Grupo de Trabajo del artículo 29 en el Dictamen 3/99, relativo a la Información del sector público y la protección de datos personales: «**El legislador, cuando desea que un dato se vuelva accesible al público no considera sin embargo que haya de convertirse en *res nullius*. Tal es la filosofía del conjunto de nuestras legislaciones. El carácter público de un dato de carácter personal, resulte de una normativa o de la voluntad de la propia persona a la que alude el dato, no priva, *ipso facto* y para siempre, a dicha persona de la protección que le garantiza la ley en virtud de los principios fundamentales de defensa de la identidad humana».**

Aún tomando la normativa actual como referencia, es posible perfilar el alcance del uso de los datos personales como fuentes accesibles al público, en estas plataformas colaborativas, que son las redes sociales online. Sin embargo, añadir que, teniendo conciencia de los riesgos y problemas respecto a la protección de datos, arriba expuestos, consecuencia de las características técnicas y de los usos y dinámicas a que dan lugar todas las herramientas allí disponibles, **el punto de mira debe estar en la necesidad de un concepto renovado de «fuente accesible al público en las comunicaciones electrónicas públicas» sean o no consideradas «servicio de la sociedad de la información». Y, conforme a ello, establecer un marco regulatorio, donde principios, derechos, excepciones y garantías, se modulen conforme a la naturaleza de estos servicios y sus dinámicas de uso, con realismo.** La tecnología jurídica puede ser una herramienta de gran utilidad en este contexto, sobre todo la llamada tecnología de la transparencia[90], que permita registrar los accesos a los datos, y conocer quién,

[90] Más arriba citada y comentada.

cómo y dónde se utilizan esos datos de acceso público aunque no libre. Tim-Berners-Lee[91] propugna la idea de «*open data*» referido, por ejemplo, a los datos que almacenan los Gobiernos. Idea de «*open data*» que se asemeja a la idea de «*open source» u «open software».*

3. PROTECCIÓN DE DATOS Y PRIVACIDAD DE LAS PERSONAS EN LAS REDES SOCIALES: DIRECTIVA DE COMUNICACIONES ELECTRÓNICAS Y PRIVACIDAD

Atendiendo a lo ya expuesto, y habiendo definido estas redes sociales online como servicios de la sociedad de la información, que se soportan a través de servicios de comunicaciones electrónicos disponibles al público, desde el punto de vista normativo se nos remite a la Directiva de los Servicios de la Sociedad de la Información, y a la Directiva sobre la privacidad y las comunicaciones electrónicas, y ambas, a su vez, a la aplicación a la Directiva 95/46, en sus disposiciones generales. Sin perjuicio de las normas de implementación o desarrollo de las mismas en el ámbito español, ya citadas, concretaremos las facultades y obligaciones de los sujetos principales de la relación jurídica[92], conforme a las Directivas. Y ello con el objeto de pulsar si estos derechos y deberes afirman estos sitios como bases o ficheros de datos privados, sometido su tratamiento a todos los términos de la Ley, o si, por el contrario, llaman a favor de su consideración como fuentes de información accesibles al público.

3.1. Proveedores de acceso: facultades y obligaciones en las redes sociales.

En general, tanto en el contexto europeo como en USA, **la exigencia de responsabilidad a los ISP (Internet Service Providers o proveedores de servicio de Internet) parece que debe seguir las dos siguientes reglas**: Primero, el proveedor que limite su función al mero transporte de los contenidos debe estar exonerado de toda responsabilidad. Segundo, los proveedores de alojamiento deben aplicar los estándares de diligencia exigibles: serán responsables sólo cuando —habiendo tenido conocimiento de la introducción de contenidos ilícitos— no hayan dispuesto medidas técnicas proporcionadas y razonables

[91] BERNERS-LEE, T., (2011), «Bernes-Lee craks open Goverment data vault» en www.pcpro.co.uk

[92] La que se establece entre el usuario y el titular del servicio de la red social online.

para su bloqueo y eliminación. En otro caso, se estaría aplicando un sistema de responsabilidad objetiva o por riesgo, que parece excesivo.[93] No obstante, cabe destacar la dificultad de distinguir por parte de éstos entre contenidos propios y ajenos, o, aunque en teoría los proveedores de servicios de acceso pueden controlar contenidos, en la práctica no es fácilmente posible, debido a la gran cantidad de datos e informaciones que manejan y su permanente mutabilidad.

Dicho lo cual, y trasladado al terreno concreto de la protección de datos personales en las comunicaciones electrónicas a través de redes públicas, el proveedor de servicio que da acceso a Internet, en su actividad de transmisión requiere y obtiene datos personales para llevar a cabo el servicio de comunicación requerido: los datos de localización y tráfico, serán tratados solo a efectos de asegurar la transmisión técnica o realizar las interconexiones, facturación o establecer la seguridad de las redes y servicios. El considerando 53 de la Directiva 2009/136/CE que modifica la Directiva 2002/58/CE, sobre la privacidad y comunicaciones electrónicas, quiere acotar el tratamiento por razones de seguridad: «el tratamiento de los datos de tráfico en la medida estrictamente necesaria para asegurar la seguridad de las redes y de la información, es decir, la capacidad de las redes o de los sistemas de información de resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad integridad y confidencialidad de los datos almacenados o transmitidos y la seguridad de los servicios conexos que dichas redes y sistemas ofrecen o hacen accesibles, por parte de los proveedores de tecnologías y servicios de seguridad cuando actúen como responsables del tratamiento de los datos, queda sujeto al artículo 7, letra f), de la Directiva 95/46/CE». Y el Supervisor Europeo de Protección de Datos (SEP) en su segundo Dictamen 2009/C128/04, expresamente sienta en el punto 77: «La medida en que los proveedores de servicios de comunicaciones electrónicas de acceso público pueden tratar legalmente datos de tráfico está regulada por el artículo 6 de la Directiva sobre la privacidad y las comunicaciones electrónicas, el cual limita el tratamiento de los datos a unos fines muy concretos, tales como la facturación, la interconexión y la promoción comercial. Este tratamiento sólo puede efectuarse en condiciones concretas, tales como el consentimiento del interesado en el caso de la promoción comercial. Asimismo, otros responsables del tratamiento, tales como los proveedores de servicios de la sociedad de la información, pueden tratar datos de tráfico con arreglo al artículo 7 de la Directiva de protección de datos, que dispone que los responsables del tratamiento pueden tratar datos personales

[93] LAGUNA DE PAZ, J.C. (2002). «Internet: aspectos de su régimen jurídico-público», en *Revista Española de Derecho Administrativo.*, Núm. 113, enero-marzo de 2002, págs. 5 a 30. p. 18.

si se cumple al menos una de las condiciones (bases jurídicas) enumeradas en el artículo, a las que también denomina fundamentos jurídicos». Asimismo los datos de localización se han intensificado, poniendo en riesgo los derechos fundamentales de los ciudadanos, y como muy ilustrativamente manifiesta el considerando 56 de la Directiva 136/2009CE. Y se lee en los artículos 2 y 3 del nuevo texto de la Directiva modificada.

Los datos de tráfico, localización, facturación o almacenamiento, deben quedar amparados por el deber de secreto, seguridad y confidencialidad, que también ampara el secreto de las comunicaciones, y que imponen concretamente los artículos 4 y 5 de la Directiva 2002/58/CE, modificada por la Directiva 2009/136/CE, de comunicaciones electrónicas y privacidad. Y en la legislación española, en la LOPD y la Ley General de Telecomunicaciones o en la Ley del Comercio electrónico, en su caso.

Dicho lo cual, es lógico que el prestador del servicio de red social online elija a conciencia el proveedor de acceso, pues de ello depende en gran medida el éxito de su negocio. Pues son los que proveen la tecnología (servidores, conectividad, ancho de banda…) a las redes sociales, garantizando el acceso a los usuarios y el soporte tecnológico del servicio en todas sus funciones. El prestador del servio y el proveedor de acceso acordarán el tipo de alojamiento o almacenamiento de datos de la plataforma social: Este alojamiento puede realizarse mediante un contrato de arrendamiento de servidor dedicado (*housing*)[94] o mediante un contrato de alojamiento de sitio *web* (*hosting*)[95], en función del tráfico previsto de la plataforma online y de las necesidades tecnológicas de la misma. El proveedor del servicio de comunicación electrónica tiene un deber de instalar medidas seguridad respecto a la transmisión y alojamiento de datos. La Directivas de comunicaciones electrónicas y privacidad lo imponen en el modificado artículo 4 a) y b)[96], sin perjuicio de las

[94] *Housing:* Este tipo de contrato regula el alojamiento del sitio web del cliente en un servidor propio del ISP y no compartido con ningún otro cliente. En la web del observatorio INTECO se puede encontrar un modelo de este contrato.

[95] También ahí se puede encontrar el modelo de contrato *hosting*: Este tipo de contrato regula la relación jurídica entre el proveedor de servicios de Internet (ISP) y el propietario de un sitio web que desee alojarlo en un servidor para que sea accesible desde Internet.

[96] Directiva 2009/136/C, art.4.b): «1bis. Sin perjuicio de lo dispuesto en la Directiva 95/46/CE/, las medidas a que se refiere el apartado 1, como mínimo: —garantizarán que solo el personal autorizado tenga acceso a los datos personales para fines autorizados por la ley—, protegerán los datos **almacenados o transmitidos** de la destrucción accidental o ilícita, la pérdida o alteración accidentales o el almacenamiento, tratamiento, acceso o revelación no autorizados o ilícitos, y —garantizarán la aplicación efectiva de una política de seguridad con respecto al tratamiento de datos personales».

disposiciones al respecto de las otras Directivas de redes y comunicaciones electrónicas[97]. A estos efectos es interesante la definición de «violación de los datos personales[98]» (art.2,h, Directiva 136)

Concretando, además de las obligaciones propias impuesta por la Ley al proveedor de servicio, éste puede actuar como un tercero al que el responsable del fichero (red social) encarga unos servicios, por los que debe responder conforme a la LOPD (artículos 3 apartados b y g, y 9.). Además, conforme a las Directivas de privacidad y comunicaciones electrónicas, hay que considerar los siguientes puntos respecto a la responsabilidad de estos proveedores:

- **Seguridad**: Sin perjuicio de disposiciones específicas, y considerando que las Directivas de comunicaciones electrónicas y privacidad no se aplican a grupos de usuarios restringidos ni redes de empresas[99], **las cuestiones relativas a las violaciones de seguridad o de datos personales, la notificación de las mismas, concretando quién notifica, a quién se notifica, y la supervisión e intervención de las autoridades nacionales de las notificaciones, son obligaciones básicas que recaen sobre el proveedor de servicio en relación con el usuario o abonado, y que excluyen, en principio, a las prestadores de servicios de la sociedad de la información. El proveedor deberá notificar la violación de datos personales a la autoridad nacional, salvo «cuando la violación de los datos personales pueda afectar negativamente a la intimidad o a los datos personales de un abonado o particular, el proveedor notificará también la violación al abonado o al particular** sin dilaciones indebidas, salvo que haya probado medidas de seguridad tecnológica de

[97] Directiva 2009/140/CE del Parlamento Europeo y del Consejo de 25 de noviembre de 2009, por la que se modifica la Directiva 2002/21/CE relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/19/CE relativa al acceso a las redes de comunicaciones electrónicas y recursos asociados, y a su interconexión, y la Directiva 2002/20/CE relativa a la autorización de redes y servicios de comunicaciones electrónicas. Así, concretamente, en el considerando 44 se afirma «La comunicación fiable y segura de la información a través de las redes de comunicaciones electrónicas resulta cada vez más esencial para la economía en su conjunto y para la sociedad en general… Por consiguiente, las autoridades nacionales de reglamentación deben garantizar el mantenimiento de la integridad y la seguridad de las redes públicas de comunicaciones…».

[98] Art.2.h) «violación de los datos personales: violación de la seguridad que provoque la destrucción, accidental o ilícita, la pérdida, la alteración, la revelación o el acceso no autorizados, de datos personales transmitidos, almacenados o tratados de otro modo en relación con la prestación de un servicio de comunicaciones electrónicas de acceso público en la Comunidad».

[99] Considerando 55 de la Directiva 2009/136/CE.

«características que convierten los datos en incompresibles para toda persona que no esté autorizada a acceder a ellos» (art. 4. apartados 1 bis., 3, 4 y 5, Directiva 136). **La condición para notificar** no sólo a la autoridad sino también al abonado o usuario es que «pueda afectar negativamente a la intimidad o a los datos personales». Y según aclara el considerando 61 de la Directiva 136: «Se debe considerar que una violación afecta negativamente a los datos y la intimidad del abonado o particular cuando conlleva, por ejemplo, fraude o usurpación de identidad, daños materiales, humillación grave o daño para la reputación, en relación con la prestación de servicios de comunicaciones electrónicas disponibles al público». **La necesidad de extender en breve estos deberes, no sólo a los proveedores de servicio de las comunicaciones electrónicas, sino también a otros sectores, como al de los prestadores de servicios de la sociedad de la información, es una demanda de la que se tiene constancia en el proceso de elaboración de las Directivas.**

- **Confidencialidad de las comunicaciones**: Estrechamente unida a la seguridad de las comunicaciones, y como secuencia lógica, hay que traer la cuestión primordial de la confidencialidad de las mismas. Seguridad, confidencialidad y secreto de las comunicaciones son diferentes instrumentos para defender, a fin de cuentas, la privacidad e intimidad de las personas, como baluartes de salvaguarda de otros derechos fundamentales. Tanto la LOPD como la Directiva 95/46, establecen el deber de secreto de los datos[100]. Sin olvidar los ya transpuestos artículos 4 y 5 —y teniendo en cuenta su modificación— de la Directiva 58/2002, en la LGT, artículos 33 a 36, hay que detenerse en el nuevo texto que recibe parte del artículo 5[101], y que afecta directamente a la privacidad e intimidad de las per-

[100] Artículo 10, LOPD «Deber de secreto: El responsable del fichero y quien intervenga en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo».

[101] Artículo 5, apartado 3: «Los Estados miembros velarán por que únicamente se permita el almacenamiento de información, o la obtención de acceso a la información ya almacenada, en el equipo terminal de un abonado o usuario, a condición de que dicho abonado o usuario haya dado su consentimiento después de que se le haya facilitado información clara y completa, en particular sobre los fines del tratamiento de los datos, con arreglo a lo dispuesto en la Directiva 95/46/CE. Lo anterior no impedirá el posible almacenamiento o acceso de índole técnica al solo fin de efectuar la transmisión de una comunicación a través de una red de comunicaciones electrónicas, o en la medida de lo estrictamente necesario a fin de que el proveedor de un servicio de la sociedad de la información preste un servicio expresamente solicitado por el abonado o el usuario».

sonas. Y, a su vez, ponerlo en contexto en el paquete de Directivas citadas de redes y comunicaciones públicas electrónicas, que imponen la confidencialidad de las comunicaciones y datos personales como condición esencial para los servicios. El nuevo texto del artículo 5 tiene por objeto la prohibición de introducir programas espías en el ordenador, *cookies* no autorizadas, o la descarga de virus a través de las redes, o a través de programas informáticos distribuidos en otros medios externos de almacenamiento de datos, como CD, CD-ROM o dispositivos USB, que pueden amenazar gravemente la esfera privada y/o íntima de la persona[102]. Independientemente de las precauciones personales de los usuarios, hay que advertir del deber del proveedor del servicio de cumplir con los principios y derechos de la Directiva 95/46. Y de su deber de facilitar información y ofrecer el derecho de negativa al usuario de forma sencilla y clara, de manera que «**las excepciones** a la obligación de facilitar información y proponer el derecho de negativa deben limitarse a aquellas situaciones en las que el almacenamiento técnico o el acceso sean estrictamente necesarios con el fin legítimo de permitir el uso de un servicio específico solicitado específicamente por el abonado o usuario»[103]. **Excepción que, aplicada a los prestadores de servicio de la red social, puede constituir casi un «cheque en blanco», teniendo en cuenta la naturaleza y el fin de estos servicios, en general**.

- **Datos de tráfico y localización**[104]**:** Retomando lo más arriba expuesto, cabe añadir algunos aspectos significativos que recoge la reforma de la Directiva. **Se deja constancia de cómo las nuevas tecnologías**[105] **han incrementado las posibilidades de identificación y localización, así los dispositivos sin contacto que utilizan radiofrecuencias, por ejemplo los RFID** (dispositivos de identificación por radiofrecuencia),

[102] En el contexto de las redes sociales online hay que recordar que lo propios usuarios pueden introducir programas informáticos y asimismo descargar virus o *cookies*, en detrimento de la esfera de privacidad del individuo que las recibe y de sus datos personales. E incluso más, todo ello puede ser iniciativa del propio proveedor del servicio de la sociedad de la información o de lo programadores que el mismo haya autorizado entrar en la red social y utilizar los datos para la creación de nuevas aplicaciones. En otras palabras, existen muchas formas y muchas técnicas en la red social online de socavar los datos personales y la privacidad, y evitar las prohibiciones legales incluso.

[103] Considerando 66 de la Directiva 2009/136.

[104] Art.6 de la Directiva 2002/58/CE, transpuesto en la Ley 32/2003, de 3 noviembre, General de Telecomunicaciones, artículo 38.

[105] Sobre todo la telefonía móvil que incorpora el acceso a Internet y todo tipo de aplicaciones y servicios.

que emplean radiofrecuencias para capturar datos procedentes de etiquetas dotadas de una identificación única, pudiendo luego transferirse estos datos a través de las redes de comunicaciones existentes. Nadie niega las bondades de estas tecnologías, pero tampoco que ponen en riesgo los derechos fundamentales de las personas y en concreto la intimidad o privacidad. Es por ello que «cuando estos dispositivos están conectados a las redes públicas de comunicaciones electrónicas o utilizan servicios de comunicaciones electrónicas como infraestructura básica, deben aplicarse las disposiciones pertinentes de la Directiva 2002/58/CE, incluidas las relativas a seguridad, datos de tráfico, y a la confidencialidad»[106]. **El proveedor de servicio queda sometido a las Directivas y sólo en la medida del cumplimiento de un fin legítimo podría utilizar dichos datos. A la aplicación del citado artículo 5, habría que añadir el nuevo apartado 3 del artículo 6** «el proveedor de un servicio de comunicaciones electrónicas disponible para el público podrá tratar los datos a que se hace referencia en el apartado 1 para la promoción comercial de servicios de comunicaciones electrónicas o para la prestación de servicios de valor añadido en la medida y durante el tiempo[107] necesarios para tales servicios o promoción comercial, siempre y cuando el abonado o usuario al que se refieran los datos haya dado su consentimiento previo. Los usuarios o abonados dispondrán de la posibilidad de retirar el consentimiento para el tratamiento de los datos de tráfico en cualquier momento».

La firme y sólida responsabilidad del proveedor de servicio que se impone en la ley se legitima históricamente por los tradicionales servicios de los operadores de telecomunicaciones, y contrasta con la posible responsabilidad del prestador del servicio de la red social, que aunque puede ser diferente o incluso concurrente, aparece ambigua, por su modelo de negocio y la naturaleza misma de estos servicios: mientras que la naturaleza del servicio resida en las relaciones humanas y sociales, y, en tanto se sustancien en Internet, dejan rastro, lo que se traduce inevitablemente en datos personales, de forma desconocida hasta el momento.

- **Consideraciones en cuanto guías de abonados**: Hay que remitirse a lo ya dispuesto en la Directiva 2002/58 y añadir lo que la Directiva de

[106] Considerando 56, Directiva 2009/136.

[107] RALLO LOMBARTE, A. (2010). «El derecho al olvido y su protección», *Revista Telos. Cuadernos de Comunicación e Innovación*. Núm. 85-octubre 2010.

Servicio Universal[108] subraya al efecto, en su nueva redacción del artículo 21, referido a transparencia y publicación de información, que en su apartado e) reza: «informar a los abonados de su derecho a decidir si incluyen sus datos personales en una guía y los tipos de datos de que se trata, de conformidad con el artículo 12 de la Directiva 2002/58/CE». Apartado que mejor se comprende en su contexto y que explica el considerando 38 de la nueva Directiva citada 136[109].

Habida cuenta que aquí se está planteando la posible categorización de las redes sociales como fuentes públicas de información, que también son estas guías telefónicas, el texto del anterior considerando puede iluminar tal propuesta, pues la interrelación de datos en la misma red social y entre ellas, y con la ayuda de otros mecanismos técnicos (como los motores de búsqueda), parece estar en sintonía con la sugerencia de un servicio de guía centralizada de abonados de todos los operadores que se dice en el abajo reproducido considerando 38.

- **Comunicaciones comerciales no solicitadas**: Con remisión a la doctrina especializada[110] que ya ha estudiado detenidamente este punto, señalar, a efectos de este trabajo, que a la prohibición de comunicaciones comerciales no solicitadas y a la prohibición del *spam,* —que para los servicios de la sociedad de la información hay que remitirse también a la Ley de Comercio Electrónico—, hay que añadir algunas novedades de la

[108] Directiva 2002/22/CE (Directiva servicio universal), modificada por la Directiva 2009/136/CE del Parlamento Europeo y del Consejo de 25 de noviembre, por la que se modifican la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y servicios de comunicaciones electrónicas,…

[109] Considerando 38 «Los servicios de consulta de números de abonado deben prestarse, y con frecuencia se prestan, en condiciones de competencia comercial, de conformidad con el artículo 5 de la Directiva 2002/77/CE de la Comisión, de 16 de Septiembre de 2002, relativa a la competencia en los mercados de redes y servicios de comunicaciones electrónicas. Las medidas aplicadas al mercado al por mayor para garantizar la inclusión de datos de usuarios finales (fijos y móviles) en las bases de datos deben respetar las salvaguardias de protección de datos personales, incluido el artículo 12 de la Directiva 2002/58/CE. El suministro de dichos datos en función de los costes a los proveedores de servicios, con la posibilidad de que los Estados miembros creen un mecanismo centralizado que facilite información completa y agregada a los proveedores de servicios de guías y la provisión del acceso a la red en unas condiciones razonables y transparentes, debe ponerse en marcha de forma que los usuarios finales se beneficien plenamente de la competencia, con el objetivo último de suprimir la regulación de las tarifas al por menor de estos servicios y de ofrecer servicios de guía telefónica con arreglo a condiciones razonables y transparentes».

[110] DAVARA RODRÍGUEZ, MIGUEL ANGEL. (2007). «La protección de datos e Internet», *Boletín del Ilustre Colegio de Abogados de Madrid. La Protección de Datos (y II).* Núm. 3. Abril, 2007. p. 222.

modificada Directiva de privacidad y comunicaciones electrónicas. Del nuevo artículo 13, a efectos de nuestro estudio, llama la atención especialmente los apartados 4 y 5. Parece muy oportuna la aplicación del apartado 4[111] en algunas prácticas de los usuarios o del prestador de servicio e incluso de terceros en las redes sociales online, aunque también hay advertir que estas plataformas ofrecen posibilidades que fácilmente eluden la ley. **La remisión a la Directiva de los Servicios de la Sociedad de la Información introduce de lleno en su ámbito a los prestadores de servicios de la sociedad de la información (y de redes sociales online).** Respecto al 5 halagar la posibilidad de que tanto la **persona física como jurídica** «que adversamente afectada por las infracciones de las disposiciones nacionales adoptadas de conformidad con el presente artículo, y por lo tanto con intereses legítimos en la cesación o prohibición de dichas infracciones, **incluidos los proveedores de servicios comunicaciones electrónicas** que deseen proteger sus intereses comerciales legítimos o los intereses de sus clientes, pueda emprender acciones legales contra dichas infracciones. Los Estados miembros podrán establecer asimismo normas específicas sobre las sanciones aplicables **a los proveedores de servicios de comunicaciones electrónicas que contribuyan por su negligencia a la comisión de infracción de las disposiciones nacionales adoptadas en virtud del presente artículo».** Conducta que puede concurrir con la del prestador de servio[112], especialmente si adicionalmente realiza servicios de comunicación electrónica, **y prestador de servicio** que, en tanto que persona física o jurídica, también puede emprender acciones contra las infracciones comunicaciones comerciales no solicitadas o el *spam* para proteger sus intereses o los de sus clientes. Igualmente, **los usuarios y terceros**, en tanto en cuanto les afecte

[111] Apartado 4 «Se prohibirá, en cualquier caso, la práctica de enviar mensajes electrónicos con fines de venta directa en los que se disimule o se oculte la identidad del remitente por cuenta de quien efectúa la comunicación, o que contravengan lo dispuesto en el artículo 6 de la Directiva 2000/31/CE, o que no contengan una dirección válida a la que el destinatario pueda enviar una petición de que se ponga fin a tales comunicaciones o en los que se aliente a los destinatarios a visitar páginas *web* que contravengan el artículo 6 de la Directiva 2000/31/CE.

[112] Pues la Directiva y la Ley del Comercio electrónico le imponen tales obligaciones también. Véase la Directiva 2000/31/CE, de 8 de Junio, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, y en particular el comercio electrónico en el mercado interior. Y su transposición en España por la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y del Comercio electrónico (LSSI-CE). Modificada en algunos artículos por la Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información.

adversamente. El Supervisor Europeo de Protección de Datos, en su citado Segundo Dictamen reflexiona al respecto «que los perjuicios infligidos a una persona considerada individualmente no son en sí suficientes, normalmente, para que emprenda una acción legal. Las personas no suelen acudir a los tribunales por su cuenta porque les envíen comunicaciones comerciales no solicitadas o porque su nombre figure indebidamente en un listín telefónico. Esta enmienda permitiría a las asociaciones de consumidores y asociaciones profesionales que representen colectivamente los intereses de los consumidores emprender acciones legales en nombre de estos ante los tribunales»[113]. **Y, efectivamente, al recoger el artículo 13.5 esa posibilidad, se han ensanchado los mecanismos de protección de las personas individuales, y, en consecuencia, para los usuarios de las redes sociales online respecto a las comunicaciones comerciales no solicitadas y el *spam.*** Sin embargo, no empece volver a repetir la misma observación más arriba hecha, y es que tanto el prestador del servicio de la red social, como los usuarios e incluso terceros, tienen resortes técnicos y realizan dinámicas de comunicación en estas plataformas, que propician bordear y dejar intactas de infracción las normas de la Directiva, al no caer sus conductas, en muchos casos, dentro de su ámbito de regulación.

3.2. Prestadores de servicio: facultades y obligaciones en las redes sociales

Los prestadores del servicio de la red social son responsables de datos en virtud de la Directiva relativa a la protección de datos, pues proporcionan los medios y servicios básicos para que los usuarios registren voluntariamente sus datos. También determinan los fines de uso y tratamientos de los datos y si pueden utilizarse con fines publicitarios o comerciales, incluida la publicidad proporcionada por terceros. A sabiendas que la prohibición de utilizar el correo electrónico con fines de comercialización directa no se aplica a las comunicaciones personales. **Los proveedores de aplicaciones** que operen en la red también pueden ser responsables del tratamiento de datos, si desarrollan aplicaciones que funcionan además de las de dispuestas por el prestador, y que el usuario decide utilizar. Estos mismos, **los usuarios** pueden resultar responsables de datos, cuando sus actividades exceden el ámbito puramente personal o

[113] Segundo Dictamen 2009/C128/04, p. 39.

doméstico: así, por ejemplo, si el usuario actúa en nombre de una empresa o de una asociación o utiliza la plataforma con fines comerciales, políticos o sociales, la exención no se aplica. Lo mismo ocurre cuando el acceso a la información del perfil va más allá de los contactos elegidos, en particular, y no conocer a muchos de ellos, o cuando todos los miembros de la red pueden acceder al perfil o cuando los datos son indexables por los motores de búsqueda, el acceso sobrepasa el ámbito personal o doméstico. Además la aplicación de la exención domestica se ve limitada por la necesidad de garantizar **los derechos de terceros,** especialmente en relación a los datos sensibles. Pero aún aplicándose, cabe la aplicación de otras disposiciones civiles o penales cuando se incurre en la violación de otros derechos. **En definitiva, la responsabilidad del prestador del servicio de las redes sociales online se encuentra sometido plenamente, vía Directiva del Comercio electrónico, a la Directiva de datos 95/46, y a la Directiva de privacidad y comunicaciones electrónicas, en algunas disposiciones. Y a fin de no ser repetitivos de lo que ya está previamente estudiado, parece oportuno remitirse al acertado Dictamen 5/2009 sobre las redes sociales en línea, del Grupo de Trabajo sobre Protección de datos del Artículo 29** (http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm), y atender a la determinación de responsabilidades que ahí se lleva a cabo, con el fin de evitar redundancias.

Y si se admite lo anterior, se puede afirmar que:

- Dado que los términos de servicio para el registro y uso son tan amplios y de finalidades tan indefinidas, el prestador tiene casi un indefinido e ilimitado uso de los mismos. A lo que hay que añadir que, por defecto, los datos del perfil del usuario, como de sus contactos y comunicaciones, son públicos y no al revés.
- Puesto que la exención domestica cede en muchos casos, el usuario es responsable de los datos que utiliza, con lo que reduce la responsabilidad del prestador.
- La Directiva 95/46, como la LOPD, que en su artículo 11.1 indica: «Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado». No obstante, este consentimiento no será preciso, según el artículo 11.2 «cuando la cesión está autorizada en una Ley y «cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros». Lo que unido al nuevo artículo 13.2[114] de la Directiva de pri-

vacidad y comunicaciones electrónicas, permite al prestador un amplio abanico casi ilimitado de usos y tratamientos de los datos, pues la relación jurídica se suele establecer en muy amplios términos, generalmente.

- La nueva redacción del artículo 5, apartado 3, de la Directiva 2009/136, establece: «Lo anterior no impedirá el posible almacenamiento o acceso de índole técnica al solo fin de efectuar la transmisión….o en la medida de lo estrictamente necesario a fin de que el proveedor de un servicio de la sociedad de la información preste un servicio expresamente solicitado por el abonado o el usuario». Disposición que también concede al prestador un amplio margen de maniobra para la utilización de los datos personales en cumplimiento de la prestación de su servicio, el cual se acuerda, generalmente, en términos amplios e imprecisos.
- El artículo 7 letra f de la Directiva de Datos dispone que los responsables puedan efectuar el tratamiento de los datos «si es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado…». Otra disposición que le concede margen de maniobra en el uso y tratamiento de datos.
- Por otra parte, las distintas excepciones, no sólo la de uso doméstico, sino otras que vienen legitimadas por fines de investigación, libertad de expresión e información, libertad de creación, etc.., dan una buen respiro, de nuevo, al prestador de servicio respecto a los datos personales que se contienen en la plataforma.
- Aunque el proveedor de servicios de comunicaciones electrónicas de redes públicas, en cuanto a la conservación de datos, está sometido a la Directiva 2006/24/CE[115], el prestador de servicios de la sociedad de la información no tiene tal imposición de conservación de los datos por un pe-

[114] Art. 13.2 «No obstante lo dispuesto en el apartado 1, cuando una persona física o jurídica obtenga de sus clientes la dirección de correo electrónico, en el contexto de la venta de un producto o de un servicio de conformidad con la Directiva 95/46/CE, esa misma persona física o jurídica podrá utilizar dichas señas electrónicas para la venta directa de sus propios productos o servicios de características similares, a condición de ofrezca con absoluta claridad a los clientes, sin cargo alguno y de manera sencilla, la posibilidad de oponerse…»

[115] Directiva 2006/24/CE del Parlamento Europeo y del Consejo, 15 de marzo 2006, sobre conservación de datos generados o tratados en relación con la prestación de servicios comunicaciones electrónicas de acceso público o redes públicas de comunicación. Y por la que se modifica la Directiva 2002/58/CE. Directiva transpuesta al Derecho español mediante la Ley 25/2007, 18 de octubre de conservación de datos de los servicios de comunicaciones electrónicas.

riodo de dos años, por razones de seguridad del Estado. El prestador, en nuestro caso del servicio de red social online, está sujeto a las normas de la Directiva de datos, y, por lo tanto, el periodo de conservación de éstos es el absolutamente necesario para el cumplimiento de sus fines (y ya se sabe que son muchos e indefinidos).

Dando un paso más, se constata más claramente que la responsabilidad[116] del prestador del servicio de red social se atenúa o vacía por arriba y por abajo, quiere decirse, en otras palabras: por las que asume el proveedor de comunicaciones electrónicas y por las que asume o se exonera el propio usuario, e incluso por los proveedores de programas informáticos.

3.3. Los usuarios y miembros: facultades y obligaciones en la red social.

Aunque este punto ya se ha atendido a lo largo del trabajo, y no resulta útil repetir lo que ya se ha traído al texto, sí se va a subrayar una idea que a modo de conclusión respecto a los usuarios y miembros de la red **puede apuntalar la hipótesis que aquí se está contemplando:** y es que si, como se está mostrando, **el usuario unas veces se mueve en el segmento legal de la exención doméstica, en cuanto a la protección de datos personales; otras, en el de las excepciones de la libertad de expresión e información; y casi siempre en el de la libre creación, con mayor o menos fortuna, por no mencionar otras que la ley recoge; y siendo verdad que todos los derechos y libertades en juego tienen que armonizarse y coordinarse, no parece, sin embargo, que pueda exigirse un estricto cumplimiento si se caracterizan como datos personales de ficheros privados, cuando estas plataformas se muestran como instrumentos tan útiles para el ejercicio de los derechos del artículo 20, y por lo tanto para la formación de la llamada opinión pública[117].**

[116] Cuestión distinta pero de gran importancia es la de la ubicación de estos prestadores fuera del espacio de la Unión Europea. Dado que la mayoría de los prestadores de estos servicios operan desde fuera de la UE (principalmente desde USA), se ha de analizar en qué medida es posible exigir a las plataformas el cumplimiento de la normativa comunitaria. La solución hay que buscarla en la LOPD 15/1999; en la LSSI, en su artículo 4. Y además son de gran ayuda los Dictámenes del Grupo de Trabajo del Articulo 29: «Dictamen sobre cuestiones de protección de datos en relación a los Buscadores» (WP148); «Documento de trabajo de trabajo relativo a la aplicación internacional de la legislación comunitaria sobre protección de datos al tratamiento de los datos personales en Internet por sitios *web* establecidos fuera de la UE» (WP56). También puede seguirse el análisis que al respecto se ha hecho en le citado: Estudio sobre la privacidad de los datos y la seguridad de la información en las redes sociales., AGEPD e INTECO.

Lessig, en su ya famoso *Code versión 2.0,* citado más arriba, realiza un elogiable esfuerzo por poner en relación en Internet derechos como el de privacidad, libertad de expresión y propiedad intelectual. Aunque él parece «redescubrir» la patrimonialización[118] de los datos personales o información privada, pone, desde su punto de vista, blanco sobre negro, para diferenciar la protección de datos personales privados y la protección de la propiedad intelectual: mientras que la propiedad intelectual no disminuye en valor una vez creada la información, difundida y compartida; la información privada, sí; cuanto más gente la conozca menos valor tiene. Y añade «*in this way, privacy is more like real property than it is like intellectual property*»[119].

No es una cuestión baladí el hecho de que sean los propios particulares, y no tanto el Estado, el origen y causa de la mayoría de las intromisiones o ataques. Además, una de las críticas de calado que se hace a la protección de la intimidad o privacidad, a través de los datos personales en estos servicios, es la falta de contexto de las comunicaciones que se exhiben en las «paredes», y cabe decir que el problema no es nuevo. Si se consideran como espacios privados de comunicación estrictamente personal, el problema es el mismo que siempre ha existido respecto a la correspondencia epistolar: el contenido y el tono de la carta puede tener un sentido cuando se escribe, pero, quizá cuando se recibe ya ha perdido parte de su sentido, y puede pasar que leídas las mismas después de cierto tiempo, ni siquiera para el que las escribió guardan significado. Quizá no sería un despropósito pensar que estos sitios son «otra cosa» diferente, y no una especie de comunicación epistolar en el ciberespacio, y que cuestionado el concepto de «dato» se puede cuestionar su conjunto. Y repensar la privacidad en el espacio público.

---

[117] YOKAI BENKLER, o.c. Son muchas las contribuciones en la bibliografía norteamericana a este debate, sobre el papel que podrían realizar las comunicaciones de Internet en la Democracia. Véase, entre otros: SUSTEIN, CASS R., (2007), *Republic.com 2.0*, Princeton, Princeton University Press. Puede resultar muy interesante el capítulo 9, en el que el autor hace sus propuestas y sugiere que en Internet también deba seguirse la doctrina «public-forum doctrine» la cual impone «a kind of must-carry rule for streets and parks», p. 190.

[118] En este aspecto, USA mira a Europa, y no al revés. Pues en la Unión Europea ya hace tiempo que se cuenta con legislación que protege no sólo los datos personales, sino también las llamadas «bases de datos» como derecho sui generis de la propiedad intelectual. No se pude olvidar que en el ámbito europeo la protección de datos personales ha sido reconocido como un derecho fundamental, y de ello se ha partido en este trabajo. Sin embargo, en USA se protegen los datos personales desde el derecho a la privacidad. Lo que no quiere decir que allí, finalmente, no sea efectiva la protección.

[119] LESSIG, L., o.c., p. 231.

En definitiva, lo que se quiere decir es que estos espacios parecen más próximos a su consideración como fuentes públicas de información, desde el punto de vista de la legislación de la protección de datos, que a su consideración como ficheros privados de datos personales. Lo que no quiere decir que deban estar desprovistos de toda protección, sino de un régimen jurídico diferente y acompasado a su naturaleza de medio de comunicación pública en Internet[120].

Además, desde esta concepción, se evitan posibles tentaciones de reivindicar el secreto de las comunicaciones, en algunos casos, y que se ejercería *erga omnes*, frente a los poderes públicos y frente a particulares[121], y atrae todas las garantías constitucionales de los derechos fundamentales[122]. La STC 114/1984, de 29 de noviembre, en su FJ 7º sienta el «secreto de las comunicaciones» como un concepto de contenido formal y no ligado necesariamente a la intimidad: «..el concepto de «secreto» en el art.18.3 tiene carácter «formal», en el sentido de que se predica de lo comunicado sea cual sea su contenido y pertenezca o no el objeto de la comunicación misma al ámbito de lo personal, lo íntimo o lo reservado». Y tal secreto cubre no sólo las comunicaciones explícitamente señaladas en el artículo 18.3 CE, sino de cualquier medio de comunicación. Luego, en principio, es extensible a las comunicaciones en Internet. Otra cosa es la naturaleza técnica de los diferentes tipos de comunicaciones, pues parece que lo ocurre en la Red no es comparable a la telefonía[123] o las comunicaciones postales. Como señala el profesor Aragón, «el bien constitucionalmente protegido es así… —la libertad de las comunicaciones, siendo cierto que el derecho puede conculcarse tanto por la interceptación en sentido estricto,… como por el simple conocimiento antijurídico de lo comunicado… Y también puede decirse que el concepto de «secreto», que aparece en el artículo 18.3, no cubre sólo el contenido de la comunicación,

[120] En los medios de comunicación convencionales, la utilización de datos personales por los medios se ve legitimada, en muchas ocasiones, por el fin de interés general informativo. Y, asimismo, la obtención y uso de los datos que en ellos se encuentran, como fuente de información de acceso público, justifica las excepciones de algunos derechos de los titulares de los datos.

[121] Un artículo esencial por contener la jurisprudencia del TRIBUNAL CONSTITUCIONAL Y DEL TRIBUNAL EUROPEO DE DERECHOS HUMANOS, de manera actualizada, y examinar la institución a su luz, pero de una forma analítica e integradora de los diferentes aspectos: ARAGÓN REYES, M., «Intervenciones Telefónicas y Postales (Examen de la Jurisprudencia Constitucional)», *Revista Teoría y Realidad Constitucional*, UNED, núm. 25. 2010.

[122] Artículos 18.3 y artículo 53 de la CE, básicamente.

[123] Véase, para su comparación: CATALÁ I BAS, ALEXANDER H. (2010). «Escuchas telefónicas. Un encuentro con el Tribunal Constitucional y un desencuentro con el legislador español», *Revista Europea de Derechos Fundamentales*, IDP, Año 2010, núm. 15.

sino también, en su caso, otros aspectos de la misma, como por ejemplo, la identidad subjetiva de los interlocutores o de los corresponsales…»[124]

Teniendo en cuenta que «no hay lesión del derecho al secreto de las comunicaciones cuando la conversación telefónica es grabada por el interlocutor o autorizada su escucha expresamente por éste»[125] o cuando la comunicación es abierta (aunque puede afectar al derecho a la intimidad), también es cierto que, en algunas redes y en algunos casos, los usuarios albergan el deseo de confidencialidad, cuando comunican con interlocutores muy concretos y reducidos. Pero incluso éstos, que podrían reclamar tal secreto, no pueden ignorar que el prestador del servicio tiene acceso a muchos datos protegidos por el derecho al secreto de las comunicaciones: identidad de los interlocutores, IP[126], tiempo de la comunicación, lugar, número y frecuencia de estas, movimientos online, número de teléfono si se ha accedido por el móvil, etc. Aunque se podría defender el carácter cerrado de las comunicaciones en la red social (desde el momento que se requiere el registro del usuario), parece más realista afirmar su carácter abierto, tanto por las interacciones de los usuarios como por los mecanismos técnicos que captan las comunicaciones y datos de la misma. Sólo el uso del *email* en la propia red social puede garantizar el derecho al secreto de las comunicaciones. Desde el momento en que el usuario, expresa o tácitamente, consiente el conocimiento y unos ciertos usos de sus datos y comunicaciones, no es fácil defender tal derecho al secreto. No sería coherente exigir el derecho y el deber al secreto de las comunicaciones a un medio de comunicación social. **Cuestión distinta, firme en la ley, es el deber de secreto de las comunicaciones de los operadores y proveedores de red**[127]**, ya estudiado.**

---

[124] ARAGÓN, M., o.c., p. 447.

[125] Esta doctrina se reitera en la STC 56/2003, de 24 de marzo. O*, contrario sensu*, en la STC 230/2007, de 5 noviembre.

[126] El Grupo de Trabajo del Artículo 29 en su «Dictamen sobre el concepto de datos personales» considera las direcciones IP como datos sobre una persona identificable.

[127] Resulta de interés el reciente Dictamen del ABOGADO GENERAL, CRUZ VILLALON, del TJUE en el asunto C-70/10. Petición de decisión prejudicial planteada por la Cour d´appel de Bruxelles (Bélgica) el 5 de febrero 2010. Scarlet Extended SA/Société Belge des Auteurs Compositeurs y E´diteurs. (2010/C 113/30). En el mismo, CRUZ VILLALÓN concluye que una medida que ordena a un proveedor de acceso a Internet que establezca un sistema de filtrado y de bloqueo de las comunicaciones electrónicas, con el fin de proteger derechos de propiedad intelectual, vulnera, en principio, derechos fundamentales. Asimismo, añade que el establecimiento del mencionado sistema de filtrado de bloqueo se configura como una limitación del derecho al respeto del secreto de las comunicaciones y el derecho a la protección de datos de carácter personal, amparados por la Carta de los Derechos Fundamentales. Del mismo modo, la instalación de tal sistema limita la libertad de información, protegida asimismo por la citada Carta.

Para finalizar, concluir que aunque el derecho a la protección de datos personales parece un «superderecho», que permite la defensa del resto de los derechos fundamentales en Internet, esto es una ilusión, por razones arriba expuestas, a las que me remito. Pues en Internet todo se traduce o materializa en datos, todo deja rastro, rastro que son datos de la persona, en definitiva. Es su naturaleza. En algunos casos su defensa es imperativo de la libertad (en relación a los proveedores y operadores de redes[128]), pero en otros habrá que atemperar su protección y sus posibilidades de protección, conforme al principio de proporcionalidad. En el mundo virtual, al igual que en el mundo real, la mejor defensa de cada derecho es a través del ejercicio y protección de cada derecho fundamental.

CONCLUSIONES

1. Las redes sociales online son servicios de la sociedad de la información que se soportan y sustancian a través de los servicios de comunicaciones electrónicas disponibles al público en las redes públicas. En materia de protección de datos y privacidad, para los servicios de redes sociales online, habrá que atender siempre a la Directiva 95/46/CE general de protección de datos y a la Directiva de los Servicios de la Sociedad de la Información, y siempre que sea posible, a aquellos artículos que sean aplicables de la Directiva de las comunicaciones electrónicas y privacidad, en los que el legislador ha querido dar entrada a otros servicios, como los servicios de la sociedad de la información.
2. La necesidad de armonización del principio de acceso a la información pública y el principio de protección de datos personales se produce tanto en el sector público como en el privado. Las excepciones que se encuentran a los derechos y principios del interesado responden a tal armonización, en aras del interés general. Las denominadas por la ley «fuentes accesibles al público» son una de las principales excepciones al consentimiento del titular de los datos, de manera que sin contar con éste se va poder tratar determinados datos en el sector privado. Las redes sociales online, como ficheros de datos privados, están sometidas al conjunto de principios y derechos que asisten al ciudadano por ley; pero también al conjunto de excepciones a los mismos, con el fin de satisfacer intereses generales, como los informativos, económicos o científicos, entre otros.

[128] Ibid.

© UNED. *Revista de Derecho Político*
N.º 81, mayo-agosto 2011, págs. 101-154

3. Centrar la protección de datos personales y privacidad en el registro del perfil del usuario, es insuficiente. El perfil es sólo la punta del iceberg, pues los verdaderos riesgos se ocultan en las aplicaciones informáticas del servicio y en otros mecanismos software, que captan los usos, comunicaciones e interacciones del usuario sin advertirle.
   El derecho a la protección de datos personales exige su replanteamiento a la luz de un renovado concepto de «dato», propiciado por las nuevas tecnologías. Por ello se duda de si es una herramienta útil para proteger el derecho fundamental a la privacidad y/o intimidad en las redes sociales. La plataforma «aplana» todos los datos a una única dimensión, sin contextualizar, a tenor de los usos con finalidades múltiples, y consecuencia del cruce de comunicaciones de contactos de muy distinta índole. En definitiva, los datos se convierten en irrelevantes para preservar la privacidad, que no tiene sentido en el sitio de la red social.
4. La posible protección de la identidad en estas redes sociales se manifiesta en una doble vertiente: impidiendo y prohibiendo la suplantación de la identidad, por un lado; y estableciendo el deber de proteger el derecho de cada usuario a que su identidad pública sea respetada tal cual él mismo ha ido construyendo, ya sea con datos concretos registrados, ya sea de los que se desprenden de sus movimientos e interacciones en la Red, por otro. La utilización de seudónimos o anónimos no parece útil, pues la identidad se puede extraer de otros datos, algunos de ellos «invisibles».
5. El usuario, salvo que se le aplique la exención de ámbito doméstico, podría ser considerado responsable del tratamiento de datos respecto al fichero que constituye su cuenta. El prestador del servicio online lo es respecto el fichero privado creado por los registros de perfiles y contactos de los usuarios e independientemente de la responsabilidad sobre los datos de tráfico, localización y conservación del proveedor de servicios de comunicación pública en Internet. Exención de ámbito doméstico en el tratamiento de datos, ficheros privados, excepciones al derecho y fuentes accesibles al público, son categorías que están implicadas en el complejo entramado de contactos, datos, informaciones e interacciones que son las redes sociales online.
6. Los verdaderos riesgos y amenazas en el cumplimiento de los principios y derechos de protección de datos del usuario, reconocidos por ley, en este servicio de la sociedad de la información, tienen un rostro invisible dibujado por el software y las diferentes aplicaciones. La capacidad de convertir datos inocuos, desestructurados y aparentemente sin sentido, en datos personales identificables es ya una realidad, que deja «tocado» el núcleo

mismo de la legislación, que es el concepto de dato personal, alrededor del cual gira toda la normativa. Normativa que, aplicada a las redes sociales online, puede requerir, consecuentemente, cambios y nuevos conceptos jurídicos. Solución que puede pasar por una nueva concepción de las redes sociales online como «fuentes de información accesibles al público» (entre las que se encuentran en la legislación vigente los medios de comunicación, boletines oficiales, las guías telefónicas o los repertorios profesionales), permitiría, ponderando el principio de proporcionalidad, una protección más adecuada de estos datos en un medio técnico como Internet, donde otros derechos, como el derecho a la información o el derecho a la libre creación, requieren también de armonización. Estas plataformas se van transformando en fuentes de información y a su vez en fuentes de fuentes de información. La riqueza, y no sólo informativa, que estas plataformas generan, sólo se debería ver limitada aplicando, rigurosamente, el principio de proporcionalidad, que mida la posible restricción de derechos individuales a favor de intereses públicos generales. Desde el momento que estos sitios se constituyen en «algo más « que ficheros o bases de datos personales, donde las libertades de información, expresión y creación, se ejercen y despliegan sin precedentes por los ciudadanos, con el consiguiente impacto en la institución de la llamada opinión pública, garantía institucional de la democracia, se requiere una nueva perspectiva jurídica.

7. Desde esta perspectiva jurídica, no resultaría «violenta» la presencia de Administraciones o Instituciones Públicas, como usuarios de estas redes. Con independencia de la llamada «Administración electrónica», su presencia potenciaría la relación directa con los ciudadanos. Sin olvidar que aquí se propone que «las fuentes accesibles al público» se repiensen, considerando, a partir de la legislación vigente, una naturaleza híbrida de las mismas, como medio de comunicación, guías telefónicas y repertorios profesionales, etc., que no coincide exactamente con ninguna de las categorías actuales.
8. En principio, cabe una conclusión más general, la responsabilidad del proveedor de redes y servicios se mantiene sólida y firme. Mientras que la del prestador del servicio de la red social, en este caso, se atenúa por arriba y por abajo: dicho de otro modo, por la que asume el propio proveedor de comunicaciones o por la que se exonera, o asume, en su caso, el propio usuario, e incluso por los proveedores de programas informáticos. La modificada Directiva de comunicaciones electrónicas y privacidad, refuerza las obligaciones y responsabilidades de los operadores y proveedores de servicios de comunicaciones electrónicas públicas. Entre las

© UNED. *Revista de Derecho Político*
N.º 81, mayo-agosto 2011, págs. 101-154

novedades, además de establecer límites más claros respecto al uso de los datos de tráfico, localización, o por razones de seguridad, se les impone el deber de comunicar a las autoridades nacionales las «violaciones de seguridad», que cuando afecten negativamente al usuario, debe ser igualmente informado. También se les legitima, junto a otras personas físicas o jurídicas adversamente afectadas (como al usuario o al prestador del servicio de la red social), a emprender acciones legales para perseguir las comunicaciones comerciales no solicitadas o el *spam*. Aunque su conducta negligente en la permisión de tales conductas puede ser sancionada por la autoridad competente.

9. Sin embargo, artículos como 5.3 de la nueva Directiva de comunicaciones electrónicas y privacidad o el artículo 11.2 de la Directiva de protección de datos, permiten tanto al proveedor de acceso, como al prestador del servicio de la sociedad de la información, que es la red social también, un margen de maniobra muy amplio en la utilización de los datos, con el fin legítimo de la transmisión o de satisfacer el servicio solicitado. Que en el caso de la red social, dado el modelo de negocio y la naturaleza misma del servicio, queda exacerbado, pues todo, al fin y al cabo, se traduce en datos en Internet.

10. En definitiva, dado el elenco de excepciones y exenciones que asisten al usuario, que confieren plena legitimidad al ejercicio libre del derecho a la información, expresión o de creación literaria, científica o técnica, estos espacios parecen más próximos a su consideración como fuentes públicas de información, desde el punto de vista de la legislación de la protección de datos, que como ficheros privados de datos personales. Lo que no quiere decir que los datos personales deban estar ahí desprovistos de toda protección, sino de un régimen jurídico diferente y acompasado a su naturaleza de medio de comunicación pública en Internet.

Title

Online social networking: open data sources or private personal data (Applying the Directives of data protection and privacy in electronic communications).

Summary

1. Introduction. 2. Statutory subject matter of online social networking sites. 3. General principle of open access to public information sources vs. general principle of protection to private personal

data sources. 4. Data protection and privacy in online social networking (Applying the Directives of data protection and privacy in electronic communications). 5. Conclusion.

Resumen

Desde la perspectiva del derecho a la protección de datos personales, los servicios de redes sociales online se muestran «resistentes» en el cumplimiento de los principios y derechos establecidos en la Ley, e incluso en una aparente legalidad. Las solución pude pasar por una concepción de las redes sociales online como «fuentes accesibles al público». Desde el momento que estos sitios se constituyen en «algo más» que ficheros o bases de datos personales, donde las libertades de información, expresión y creación, se ejercen y despliegan sin precedentes por los ciudadanos, con el consiguiente impacto en la institución de la llamada opinión pública, garantía institucional de la democracia, se requiere un cambio de enfoque.

Abstract

When one looks at the concept of using online social networking as a personal database from the perspective of data protection law issues, a number of problems arise, not least of which is identity theft. However, when one takes into account several rights, such as freedom of information and expresión or intellectual property, in addition to personal data protection, a new legal perspective seems to be required. By considering those social network services as public, open data sources, it is possible to harmonize all of these seemingly contradictory rights and laws. Furthermore, the processing of personal data from public souces has traditionally been privileged in data protection and privacy legislation.

Palabras clave

Redes sociales en Internet. Protección de datos en Internet. Fuentes de información pública. Privacidad electrónica. Derecho de Internet. Libertad de expresión e información en Internet.

Key words

Online social networking. Open data. Data protection on Internet. Public information sources. E-privacy. Internet law. Freedom of speech.