LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL EN EL ÁMBITO DE LAS REDES SOCIALES ELECTRÓNICAS: EL VALOR DE LA AUTORREGULACIÓN

David López Jiménez
Becario de investigación del Ministerio de Educación y Ciencia. Programa FPU
Universidad de Sevilla

Resumen: Las nuevas tecnologías han irrumpido en numerosos ámbitos de la vida cotidiana. Uno de los espacios en el que tales novedades técnicas operan, de manera ciertamente exitosa, es el de las relaciones sociales. En efecto, como en el presente estudio veremos, las redes sociales electrónicas suponen un destacable avance con sugerentes proyecciones tanto en el plano de la amistad como en el mundo profesional. En todo caso, se suscitan notables problemas a efectos de la protección de los datos de carácter personal. Una herramienta por la cual está última cuestión puede resolverse, de forma extraordinariamente satisfactoria, es en virtud de la autorregulación.

Palabras clave: "autorregulación"; "códigos de conducta"; "Internet"; "privacidad"; "redes sociales".

Abstract: The new technologies have popped in numerous ambiences of the everyday life. One of the spaces in which such technical innovations operate with certain success, is social relations. In effect, as we can see in the present study, the electronic social networks suppose an outstanding advance with several projections both in friendship and in the professional ambiences. In the other hand, notable problems emerged in the field of personal data protection. A tool by which these problems can be solved, in an extraordinarily and satisfactory form, is by virtue of the self-regulation.

Keywords: "self-regulation"; "codes of conduct"; "Internet"; "privacy"; "social networks".

SUMARIO: I. INTRODUCCIÓN. II. REPERCUSIÓN DE INTERNET EN EL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL. III. LA PRIVACIDAD Y LAS REDES SOCIALES. 1. Concepto de red social. 2. Modalidades de redes sociales. 2.1. Redes sociales de ocio. 2.2. Redes sociales profesionales. 3. Prácticas potencialmente invasivas de la privacidad. 4. Especial consideración de los menores de edad e incapaces. IV. LA AUTORREGULACIÓN COMO ESTRATEGIA ORDENADORA IDÓNEA DE LAS ACTIVIDADES QUE SE DESARROLLAN EN LA RED. 1. Consideraciones previas. 2. Situación imperante en materia de comercio electrónico. 3. Escenario vigente y perspectivas de futuro por lo que a las redes sociales se refiere. V. CONCLUSIONES. BIBLIOGRAFÍA.

I. INTRODUCCIÓN

El desarrollo de las tecnologías de la información y las comunicaciones (TIC) en la segunda mitad del siglo pasado ha traído consigo el surgimiento de nuevas posibilidades para la sociedad. El mundo de la empresa, la Administración Pública o la propia transmisión del conocimiento han experimentado transformaciones radicales y están abocadas a una evolución constante en el futuro más inmediato. El nacimiento de las redes determina nuevos modos de hacer, cambios en las relaciones sociales o el inicio de comunidades humanas que eran totalmente impensables hasta hoy.

Aunque las nuevas tecnologías comportan, como regla general, numerosas ventajas para el público potencialmente destinatario de las mismas, en ocasionen, todo hay que decirlo, se plantean ciertos problemas como consecuencia del uso indebido que de las mismas se hacen. Un ejemplo que al respecto puede apuntarse es el de las redes sociales y los potenciales problemas de privacidad que pueden suscitarse[1].

Antes de ocuparnos, con detenimiento, del último extremo apuntado que, dicho sea de paso, será el núcleo de la presente investigación conviene realizar unas breves consideraciones en torno a la privacidad.

Hace ya una década determinó el presidente y cofundador de *Sun Microsystems*, Scott McNEALY, que debemos ser conscientes de que no

[1] SMITH (1993): 7.

tenemos privacidad[2]. Matizando tal afirmación, posteriormente, ha llegado a afirmar, a juicio de cierto sector de la doctrina[3] de manera igual de descorazonadora, que si gozamos de privacidad es porque alguien tolera que la tengamos. Hay quien[4], incluso, ha llegado a manifestar que un exceso de privacidad podría ser contraproducente para la sociedad, proponiendo un concepto comunitario de privacidad aboga por un mayor peso del interés general. En todo caso, debe quedar muy claro que, como en el presente estudio veremos, nos encontramos en un ámbito en el que la dignidad y la libertad están en juego. Para ello hay que defender con convicción, en virtud de la ley y de la autorregulación, la privacidad. Es intolerable tener que soportar una pérdida del nivel de protección de datos de carácter personal como consecuencia de la implantación de las nuevas tecnologías.

En cuanto al concepto de privacidad no parece sencillo dar, *a priori*, una definición de lo que debe entenderse por tal. Este es un extremo que ha puesto de manifiesto tanto la doctrina[5] como la propia jurisprudencia[6]. Una definición muy extendida, aunque ya superada, es la que a finales del siglo XIX pronunció el juez americano Cooley[7] que manifestó que privacidad es el derecho a estar solo, a estar en paz ("*the right to be alone*").

La definición concreta que al respecto se enuncie dependerá, en gran medida, de la denominación específica que se haya acuñado para determinar el derecho al que nos referimos: la protección de datos de carácter personal. Lo importante, más que el *nomen iuris*[8], es que nos hallamos en el ámbito de un derecho fundamental cuyo contenido jurídico está formado por los diferentes instrumentos que integran la protección de los datos de carácter personal que posee un núcleo o reducto indisponible incluso para el legislador[9].

[2] Tales declaraciones se hicieron muy célebres sobre todo en los países de corte anglosajón y fueron puestas de relieve por un importante número de autores. Así, entre otros muchos, por BERGMAN (2000): 19; JENSEN (2002): 156; SOLOMON (2003): 223; SOLOVE (2004): 224; BENNET y RAAB (2006): 298; HAROLD y KRAUSE (2007): 2764.

[3] PIÑAR MAÑAS (2008a): 5.

[4] ETZIONI (1999): 7 y 278.

[5] GELLMAN (1998): 193.

[6] Así lo ha determinado el Tribunal Europeo de Derechos Humanos en la sentencia de 28 de enero de 2003 –asunto Peck contra Reino Unido-.

[7] COOLEY (1888): 29.

[8] GUERRERO PICÓ (2006): 187-190; REBOLLO DELGADO (2008): 37-43.

[9] LUCAS MURILLO DE LA CUEVA (1999): 39.

La irrupción de las nuevas tecnologías de marcado carácter social –*blogs*, *wikis*, *podcast*, redes sociales, etc.- ha determinado un alto grado de interconectividad entre los usuarios de Internet lo que, dicho sea de paso, les permite intercambiar todo tipo de opiniones sobre diferentes productos y experiencias con otras personas. La llegada de la *Web* 2.0 ha supuesto una revolución, pues el potencial usuario adquiere un nuevo papel dentro del soporte, ya que deja de ser un mero espectador de contenidos para ser el que elige, el que participa e, incluso, el que crea esos contenidos. En suma, la *Web* 2.0 es una *Web* más colaborativa[10] que permite a sus usuarios acceder y participar en la creación de un conocimiento ilimitado y, como consecuencia de esta interacción, se generan nuevas oportunidades de negocio para las empresas. Siendo tal circunstancia una realidad, debemos reconocer que nos encontramos ante un escenario sometido a frecuentes violaciones de la privacidad. Tal extremo resulta apreciable en los diferentes escenarios en los que se traduce la *Web* 2.0: redes sociales, *blogs* y *wikis*. En el presente estudio nos limitaremos al análisis de la privacidad en el ámbito de las redes sociales, poniendo de manifiesto las extraordinarias bondades que la autorregulación, materializada en códigos de conducta[11], ostenta.

II. REPERCUSIÓN DE INTERNET EN EL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

En la era electrónica existe una considerable preocupación por el derecho del individuo a la intimidad[12]. La sensación de libertad que el potencial consumidor o usuario experimenta en materia de comercio electrónico únicamente puede calificarse de falaz pues es simple apariencia. En efecto, no es consciente de que cualquier actividad que acometa

[10] La actividad colaborativa que comentamos se manifiesta tanto en la forma como en el contenido del servicio de que se trate –ya sea, en el ámbito de la *Web* 2.0, *blog*, red social o *wiki*-. En otras palabras, en virtud de las motivaciones personales que en cada caso concurran, el usuario podrá modificar tanto el contenido –añadiendo, cambiando o borrando información así como asociando datos a la información existente- como la forma de presentar los datos que desee mostrar en su perfil.

[11] Debe apuntarse que la autorregulación, en la *Web* 2.0, no sólo opera en el ámbito de las redes sociales sino también en los *blogs*. En relación a éstos últimos, cabe determinar que los códigos de conducta constituyen un elenco de buenas prácticas que persiguen fomentar conversaciones constructivas que respeten las formas personales de expresarse limitando la mala educación y a las actitudes incivilizadas.

[12] CASTILLO JIMÉNEZ (2002): 21-37; OLIVIER LALANA (2002): 1539-1546; PRIETO ANDRÉS (2002): 1710-1713; MARTOS (2005): 79-91; RODRÍGUEZ CÁRCAMO (2005): 1725-1751; ACEDO PENCO (2006): 97-117; ARENAS RAMIRO (2006).

en el mundo electrónico deja rastros que podrán seguirse[13] y que, en ocasiones, serán aprovechados con fines ciertamente espurios[14].

Los datos de carácter personal, en la actualidad, tienen un extraordinario valor[15]. En este sentido, los perfiles constituidos se compran y se venden a un precio nada desdeñable y, lo peor de todo, se trata de una actividad invasiva de nuestra intimidad pues, en muchas ocasiones, no habrá resultado, en absoluto, conocida ni, mucho menos, consentida[16].

Podemos entender por dato personal[17] aquella información sobre una persona física identificada o identificable (art. 2 de la Directiva 95/46/CE sobre Protección de Datos Personales, art. 3 la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal –LOPD- y art. 5.1.f) Reglamento de desarrollo LOPD –aprobado por RD 1720/2007 de 21 de diciembre-). Lo más significativo es que los datos se refieran a una persona identificada o identificable, con independencia de que el dato se refiera a uno mismo o a un tercero[18].

Las políticas de privacidad realizadas por parte de los prestadores de servicios de la sociedad de la información que operan en Internet en múltiples escenarios, en el que, naturalmente, debe entenderse incluido el relativo a las redes sociales, constituyen uno de los puntos jurídicos relevantes que deben ser tenidos en consideración para desarrollar numerosas actividades susceptibles de ser conceptualizadas en el ámbito de la publicidad interactiva, la contratación electrónica y otras muchas conexas con las mismas. Su importancia va mucho más allá del simple cumplimiento de la legalidad vigente. En efecto, con las mismas no se trata únicamente de garantizar el cumplimiento de un conjunto de obligaciones normativas pues su contenido, en numerosas ocasiones, va más allá de las mismas cubriendo un cierto vacío legal. Tal extremo puede vincularse, no sólo a la labor de promoción que el legislador efectúa por lo que a la autorregulación respecta –de la que la política de privacidad es una manifestación- que veremos en el cuarto apartado del presente estudio, sino a que las propias empresas valoran, de manera importante,

[13] LANGHEINRICH (2001); BALLESTEROS MOFFA (2005).
[14] ÁLVAREZ-CIENFUEGOS SUÁREZ (1999).
[15] MUÑIZ CASANOVA y ARIZ LÓPEZ DE CASTRO (2004): 85-118.
[16] SERRA RODRÍGUEZ, (2000).
[17] De acuerdo con la STS de 31 de octubre de 2000, el concepto de "dato personal" no es sinónimo del de "dato de carácter personal", no sólo porque no siempre un dato personal es un dato de carácter personal, sino, además, porque existen datos de carácter personal que no son datos personales.
[18] ROSSNAGEL (2003): 112.

la preocupación que los ciudadanos en general manifiestan respecto a su privacidad[19].

El Consejo de Europa[20] primero y el ordenamiento jurídico comunitario[21] posteriormente han desarrollado un completo acervo normativo que incorpora un conjunto de reglas dirigidas a garantizar los derechos individuales en el ámbito de la protección de datos. Tales normas, que contribuyen a la creación de un verdadero mercado europeo que facilite el libre intercambio de personas, mercancías, servicios y capitales, no sólo se encuentran en Directivas comunitarias[22] de notable relevancia, ya que fueron incluidas en el artículo II-68[23] del Tratado por el que se establecía

[19] JULIÁ-BARCELÓ, MARTÍNEZ MARTÍNEZ y PANIZA SULLANA (2008): 5.

[20] Procede, entre otros muchos, citar el Convenio del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, ratificado por España el 27 de enero de 1984. Tal Convenio, precisamente, surgió de la necesidad de profundizar en la protección de los derechos de los individuos respecto al uso de la informática, en especial en lo que a la vida privada se refiere, protegida por el art. 8.1 del Convenio Europeo de Derechos Humanos. Respecto a esta última cuestión nos remitimos a las consideraciones de ARENAS RAMIRO (2003): 576-580.

[21] En el marco de la Unión Europea, el art. 8 de la Carta Europea de Derechos Fundamentales reconoce, de manera expresa, la autonomía del derecho a la protección de datos que, en consecuencia, ha de distinguirse del derecho a la vida privada que comprende tanto el derecho a consentir, como el derecho de tratar los datos lealmente y de satisfacer los derechos de los afectados encomendando su tutela a su tutela a autoridades independientes. Aunque no tiene valor normativo, por lo que a nuestro ámbito de estudio respecta, debemos destacar la Comunicación de la Comisión al Parlamento Europeo y al Consejo, de 2 de mayo de 2007, sobre el fomento de la protección de datos mediante las tecnologías de protección del derecho a la intimidad (PET). Se entiende por PET, a efectos de la citada comunicación, un sistema coherente de medidas de TIC que protege el derecho a la intimidad suprimiendo o reduciendo los datos personales o evitando el tratamiento innecesario o indeseado de datos personales, sin menoscabo de la funcionalidad del sistema de información.

[22] Así, entre otras, deben mencionarse las siguientes: 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; Directiva 97/7/CE, del Parlamento Europeo y del Consejo, de 20 de mayo de 1997, relativa a la protección de los consumidores en materia de contratos a distancia; Directiva 2000/31/CE, de 8 de junio, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior; 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, (más conocida como Directiva sobre la privacidad y las comunicaciones electrónicas); Directiva 2006/24/CE, del Parlamento Europeo y del Consejo, de 21 de febrero de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones por la que se modifica la Directiva 2002/58/CE –de reciente transposición a la legislación nacional por la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones-.

[23] Tal precepto determina que "1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan; 2. Estos datos se tratarán de modo leal, para fines concre-

una Constitución para Europa que, como es sabido, fue sustituido por el Tratado de Lisboa de 13 de diciembre de 2007[24].

España ha incorporado esta área del acervo comunitario a través de la LOPD así como por el Reglamento de desarrollo –aprobado por Real Decreto 1720/2007 de 21 de diciembre-. En nuestro Ordenamiento la protección de datos ostenta la naturaleza de derecho fundamental. Así, como es sabido, el Tribunal Constitucional estableció la existencia de un derecho fundamental a la protección de datos personales en sentencias dictadas a lo largo de un decenio –desde la STC 254/1993 a la STC 292/2000[25]- fundamentándolo en el art. 18.4 de la Constitución Española.

III. LA PRIVACIDAD Y LAS REDES SOCIALES

El derecho fundamental a la protección de datos, regulado específicamente en el art. 18.4 de la Constitución Española, que ha de diferenciarse[26] del derecho a la intimidad del art. 18.1 CE (con el que guarda la similitud de ofrecer una especial protección constitucional de la vida privada, personal y familiar), atribuye a su titular un conjunto de facultades que esencialmente imponen a terceros la realización u omisión de determinados comportamientos cuya concreta regulación debe establecer la ley. Como bien determina la STC 292/2000, el derecho que sometemos a examen atribuye a su titular la facultad de "controlar el uso que se realice de sus datos personales, comprendiendo, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquél legítimo que justificó su obtención". En este sentido, por lo que a nuestros efectos respecta, cabe indicar que, desde hace varias décadas[27], se ha constatado que quienes tienen la sen-

tos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a obtener su rectificación; 3. El respeto de estas normas estará sujeto al control de una autoridad independiente".

[24] En virtud del art. 2 de la Ley Orgánica 1/2008, de 30 de julio, por la que se autoriza la ratificación por España del Tratado de Lisboa, las normas relativas a los derechos fundamentales y a las libertades que la constitución reconoce se interpretarán también de acuerdo con lo dispuesto en la Carta de los Derechos Fundamentales de la Unión Europea.

[25] Como dispone CALVO ROJAS (2008): 9, no es fácil calibrar la incidencia de esta sentencia, si bien parece indudable que todos los mecanismos de protección previstos en la LOPD recibieron con ella un vigoroso respaldo.

[26] Así lo determina, entre otros muchos, DÍAZ ARIAS (2008): 9-12.

[27] TOLCHINSKY, MCCUDDY, ADAMS, GANSTER y FROMKIN (1981): 308-312.

sación que mantienen el control sobre el uso que se hace de sus datos personales, después de haberlos facilitado a un tercero, perciben una menor invasión de su privacidad que quienes pueden tener la sospecha de que han perdido el control sobre los mismos[28]. La posibilidad de controlar nuestra propia información excluye, por supuesto, el control por otros. Cada persona debe poder controlar el grado de privacidad que desea tener y hasta dónde quiere llegar sin que, en modo alguno, sean admisibles injerencias injustificadas[29].

La progresiva importancia de estos espacios sociales electrónicos, como son las redes sociales, no está exenta, en modo alguno, de riesgos o posibles ataques malintencionados. Estamos, en este sentido, presentes ante una preocupación de las organizaciones nacionales, europeas e internacionales con competencias en las materias afectadas por el uso de las redes comentadas, que han impulsado la elaboración de normas y recomendaciones para garantizar el acceso seguro de todos los usuarios, con especial atención de menores de edad incapaces, a estos nuevos instrumentos virtuales de interacción[30].

Las principales iniciativas reguladoras en el plano comunitario provienen tanto de la Comisión Europea como del Grupo de Trabajo del Artículo 29 que recientemente ha realizado, en la Opinión 5/2009, de 12 de junio, ciertas manifestaciones en relación a la privacidad y a la seguridad de las redes sociales, sitios *Web* colaborativos y demás medios de interacción de usuarios en Internet. Es muy probable que, en virtud de las últimas declaraciones de la Comisión Europea, durante el segundo semestre de 2009 o el primero de 2010 tengamos un código de conducta que reglamente, con rigor y a escala europea, toda la materia que comentamos.

La necesidad de regular tanto en virtud de normas legales como, por efecto de estas últimas, por medio de acuerdos privados (que tomarán la forma de códigos de conducta), la protección de datos de carácter per-

[28] Para, precisamente, evitar, en primer lugar, el tratamiento de datos personales por parte de los buscadores de Internet y, posteriormente, por parte de terceros sería recomendable que las propias plataformas en las que se fundamentan las redes sociales incluyeran las modificaciones pertinentes en el código HTML de la aplicación, impidiendo, de esta manera, que los motores de búsqueda puedan indexar los perfiles de los usuarios pues estos últimos deben previamente aceptarlo. Con esta última acción, se garantiza un mayor control de la información publicada.

[29] PIÑAR (2008a): 11.

[30] Nos encontramos ante un aspecto destacado por el *Multi-State Working Group on Social Networking of State Attorneys General of the United States* que, el 31 de diciembre de 2008, ha hecho público el estudio cuyo título es *Enhancing Child Safety & Online Technologies*.

sonal en el ámbito de las redes sociales estriba, entre otros factores, en la extraordinaria importancia de las materias que abordamos. En otras palabras, teniendo en consideración, por un lado, el importante volumen de datos personales que los usuarios –menores y mayores de edad- publican en sus perfiles (que, dicho sea de paso, se erigen en verdaderas identidades digitales que facilitan un rápido conocimiento de sus datos de contacto, preferencias y hábitos[31]) y los riesgos a los que quedan expuestos, resulta aconsejable una estrecha colaboración entre las autoridades públicas y los sujetos de carácter privado que, aunando esfuerzos, coincidan en la necesidad de abordar, de forma conjunta y contundente, la protección integral de la privacidad en el ámbito de las redes sociales. De todo ello nos ocuparemos, de manera exhaustiva, en el apartado cuarto del presente estudio.

A continuación, analizaremos el concepto de red social, sus modalidades, los riesgos concretos que, a efectos de privacidad, potencialmente existen así como los momentos críticos en los que podrán plantearse más perjuicios para la protección de datos de carácter personal. También estudiaremos las medidas establecidas por parte del legislador para garantizar un mayor grado de protección de la privacidad de colectivos especialmente vulnerables como los menores de edad y los incapaces.

1. Concepto de red social

Aunque estamos ante un fenómeno relativamente reciente su avance es sencillamente imparable. El origen de tales herramientas de interacción puede cifrarse en 1995, cuando Randy Conrado crea el sitio *Web Classmates* para mantener o recuperar el contacto con antiguos compañeros de estudio –colegio, instituto, universidad, etc.-. Posteriormente (1997), nacen otras como *SixDegress*. En 2002, surgen espacios virtuales que promocionan las redes de círculos de amigos en línea adquiriendo una contrastada popularidad en 2003 con los conocidos *MySpace*, *Hi5*, *SeconLife* y *Xing*. Desde la aparición de estas últimas han nacido otras no menos importantes, en nuestro ámbito de estudio, como *Orkut* (2004), *Yahoo¡360º* y *Bebo* (2005), *Facebook*, *Twitter* y *Tuenti* (2006) y, más recientemente, *Lively* (2007).

[31] Tal extremo es puesto de manifiesto por el Instituto Nacional de Tecnologías de la Comunicación (2009): 11.

El número de usuarios de tales plataformas de comunicación crece a un ritmo, sencillamente, de vértigo[32]. En este sentido, existen redes sociales, como *Facebook*, en las que ya existen más de 200 millones de usuarios y con su *chat* supera la barrera de los 1000 millones de mensajes electrónicos diarios. Otro dato que, a este respecto, podemos poner de relieve, a tenor de ciertos estudios de carácter empírico[33], es que dentro de las primeras veinte posiciones de los 500 sitios *Web* más visitados a nivel internacional existen cuatro redes sociales cuales son *Facebook*, *MySpace*, *Hi5* y *Orkut*. Seguidamente esbozaremos ciertas notas de la interesante figura que examinamos para, posteriormente, efectuar una definición.

El modelo de crecimiento de tales redes se basa en un en un proceso viral[34] en el que un número inicial de participantes, a través de el envío de invitaciones por medio de correos electrónicos[35], ofrece la posibilidad de unirse a su sitio *Web*.

Asimismo, cabe indicar que los servicios que comentamos se erigen en poderosos canales de comunicación e interacción que permiten que los usuarios puedan actuar como grupos segmentados. Son, además, un importante instrumento para la concertación de actividades sociales de distinta índole.

Antes de dar una definición de red social conviene apuntar que nos encontramos ante un fenómeno sobre el que no existe una definición aceptada de manera unánime. En otras palabras, existen tantas defini-

[32] Según el estudio *Power to the people social media*, realizado en el primer semestre de 2008, el número de usuarios de redes sociales, a nivel mundial, puede cifrarse en 272 millones de personas. Tal dato en el caso de España, según la memoria elaborada por *Universal McCann* (2008), se sitúa en 7.850.000 usuarios.

[33] Cabe citar, en este sentido, el estudio realizado, en noviembre de 2008, por Alexa Internet, compañía parte del Grupo Empresarial Amazón, que, dicho sea de paso, constituye uno de los referentes por lo que a la medición y análisis de tráfico en Internet se refiere.

[34] Cuando hablamos de viralidad en el ámbito de las redes sociales, extrapolando a tal plataforma un concepto propio del marketing viral, nos referimos a la capacidad que tales redes ostentan para, precisamente, lograr, en el menor tiempo posible, el mayor crecimiento potencial en número de usuarios. Sobre esta cuestión nos remitimos a ROSEN (2006); LIN y SUN (2005).

[35] Debe insistirse en que el usuario puede hacer uso del servicio ofrecido por la red social en virtud del que, previa revelación de su dirección de correo electrónico y de la contraseña asociada al mismo, la plataforma accederá a su libreta de direcciones con una doble finalidad. Por un lado, conocer los contactos que ya están registrados en la red social y, por otro, remitir a todos sus contactos un correo comercial para que se registren y entren en contacto con el usuario que, precisamente, ha realizado el registro. La Agencia Española de Protección de Datos (AEPD), entre otros documentos en la memoria anual de 2008, ha determinado, en los casos en los que la comunicación tiene formato y contenido eminentemente comercial, que si la dirección IP desde la que se remite es la de la propia plataforma y si quienes la reciben no han prestado su consentimiento expreso a tal respecto nos encontraríamos ante un supuesto de comunicación electrónica no solicitada –*spam*-.

ciones como autores se han ocupado del particular. De hecho, antes de definir tal fenómeno debemos acotar el tipo concreto de red de que se trata por lo que debe diferenciarse si nos encontramos ante una red social tradicional[36] o ante una red social virtual. Debe, en cualquier caso, partirse de la premisa de que una red social ante todo es una forma de interacción entre miembros y/o espacios sociales.

Podemos, en todo caso, definir las redes sociales electrónicas como servicios prestados a través de Internet, accesibles a través de diferentes instrumentos técnicos –ordenador, teléfono móvil[37], PDA, etc.- que posibilitan que los usuarios puedan diseñar un perfil, en el que harán constar determinada información personal –texto, imágenes o vídeos-, en virtud del que podrán interactuar con otros usuarios y localizarlos según los datos incluidos en aquél.

2. Modalidades de redes sociales

Los criterios en base a los cuales las redes sociales pueden clasificarse son ciertamente numerosos ya que podrían, a tal respecto, valorarse parámetros de diferente índole como, entre otros, de tipo cronológico, territorial, el contenido que incluyen, finalidad para la que han sido diseñadas o el público potencialmente destinatario. El factor por el que, en el presente estudio, optaremos para distinguir la tipología de redes sociales que, en la actualidad, existen es el tipo de contenido presente en las mismas. A tal efecto, podemos diferenciar entre, por un lado, redes generalistas o de ocio y, por otro, redes profesionales sin perjuicio de que las primeras, a su vez, pueden subclasificarse en distintas categorías.

Antes de ocuparnos de cada una de ellas debemos advertir, de forma en todo caso breve, la concurrencia, en los dos tipos de redes descritas, de caracteres comunes. Así, las dos modalidades tienen como fin primordial poner inicialmente en contacto a distintas personas. La forma en

[36] Se entiende por red social tradicional el conjunto de personas que conocemos, con las que guardamos una relación personal más o menos estrecha y con las que, con cierta frecuencia, nos relacionamos.

[37] Merced a que el dispositivo móvil ofrece la sensación de inmediatez o de "contacto constante" entre los usuarios, este modelo de negocio –las redes sociales accedidas por teléfono móvil- se ha convertido en uno de los más exitosos. Aunque la gran mayoría de redes sociales virtuales permiten operar tanto a través de Internet (*Facebook, Meetic* o *MySpace*, entre otras) como por teléfono móvil –a través de determinados programas para estos últimos- existen plataformas específicamente diseñadas para los terminales móviles (caso de la japonesa *Mobagay Town*).

la que esto último se logrará será en virtud de una invitación operada por el emisor que, necesariamente, habrá de ser aceptada por el receptor. Tales plataformas posibilitan la interacción entre los usuarios, ya sea, por ejemplo, compartiendo información, facilitando el contacto directo entre los usuarios, etc. A partir de aquí las posibilidades de comunicación son ilimitadas.

Asimismo, debe insistirse en que en las redes sociales de ocio son, en cierta medida, por la tipología de datos personales que contienen, más susceptibles de padecer la vulneración de la privacidad de sus usuarios. En efecto, en el caso de las redes sociales generalistas, a diferencia de las que presentan carácter profesional, los usuarios exponen no sólo sus datos de contacto –dirección postal y electrónica, teléfono, etc.- sino que pueden hacer públicas sus preferencias personales en numerosos ámbitos lo que supone que el número y la categoría de datos personales que se ponen a disposición de todo interesado es notablemente mayor, insistimos, que en las redes sociales profesionales.

2.1. Redes sociales de ocio

Su objetivo prioritario estriba en facilitar y potenciar las relaciones personales entre los usuarios que representan su público real o potencial –en alusión al grupo de individuos que, en el futuro, formen parte de la red social en cuestión-. Las redes sociales generalistas que son las que, en este apartado examinamos, son susceptibles de ser subclasificadas, teniendo en consideración su finalidad, en tres categorías.

Redes sociales creadas para el intercambio de información. Posibilitan la inclusión de determinados contenidos –fotografías, vídeos, textos- que podrán ser visionados por quien, en principio, lo desee. Ahora bien, previo registro, permitirán que los interesados puedan operar ciertos comentarios en relación a los mencionados contenidos y, en ciertos casos, otorgar puntuaciones. Cabe citar, a título de ejemplo, *Youtube*, *Dalealplay.com* y *Google Vídeo*.

Redes sociales fundamentadas en perfiles. Esta subcategoría de red social suele estar dirigida a temáticas concretas erigiéndose, de este modo, en poderosas fuentes de información sobre una determinada materia. Nos encontramos, con toda seguridad, ante el tipo de red social que más se utiliza en la actualidad. Entre los ejemplos que, sobre el particular, podemos destacar merecen mención especial los siguientes: *Facebook*, *Tuenti*, *Hi5*, *MySpace*, *Wamba*, *Orkut*, etc.

Redes sociales de *microblogging*. En este caso, los usuarios escriben comentarios sobre las actividades que, en cada momento, están realizando. Tales apreciaciones, efectuadas por el titular del espacio, serán editadas tanto en su propio perfil como en el de sus contactos. Estas plataformas integran sistemas de alertas a través de correo electrónico y *SMS*. En esta concreta modalidad podemos enunciar, entre otras muchas, *Twitter*, *Tumblr* y *Yammer*.

2.2. Redes sociales profesionales

Esta tipología de redes sociales constituye una interesante herramienta para establecer contactos profesionales con otros usuarios. Los datos personales que en tales plataformas suelen hacerse constar son, además de los de carácter estrictamente académico, de contrastado perfil profesional ya que se podrán hacer figurar las distintas empresas, así como el período de tiempo, para las que se han prestado servicios profesionales. Por lo que a la presente modalidad de red social respecta debemos citar, sin ánimo exhaustivo, *Xing*, *Plaxo*, *Linkedin* y *Ryze*.

3. Prácticas potencialmente invasivas de la privacidad

En materia de protección de datos de carácter personal es donde, precisamente, acontece el mayor número de situaciones potencialmente desfavorables para los derechos de los usuarios, ya que las redes sociales fundamentan sus contenidos en los perfiles que, con relativa periodicidad, los titulares de los mismos dan de alta y actualizan.

Es observable que, a nivel legislativo, tanto en el plano nacional como comunitario e internacional, no se reglamentan, de forma específica, determinadas situaciones realmente complejas que pueden llegar a plantearse como consecuencia del uso de las redes sociales y sitios *Web* de carácter colaborativo. La mencionada ausencia de regulación legal –de diferente alcance territorial (nacional, comunitaria e internacional)- unida a la vertiginosa e imparable evolución de los servicios de la Sociedad de la Información puede dar lugar a escenarios que pongan, de una u otra manera, en duda la defensa de los derechos de los usuarios. Por lo que se refiere a los momentos en los que el potencial usuario puede ver comprometida su privacidad al recurrir a las redes sociales cabe distinguir los tres siguientes:

Al efectuar el alta, dado que, por un lado, existe la posibilidad de que el nivel de seguridad del perfil, a efectos de privacidad, no se config-

ure correctamente por lo que determinados datos[38] considerados especialmente sensibles podrían, con relativa facilidad, ser objeto de vulneración dado que los mismos–propios y de terceros (ya que también serían visibles ciertos datos de los contactos)- serían accesibles por cualquier persona potencialmente interesada[39]. Por otro lado, debe tomarse conciencia de que, como consecuencia de la aceptación de las condiciones de registro por parte del usuario, algunas redes sociales entienden otorgada la cesión, plena e ilimitada, sobre todos los contenidos propios que, de manera voluntaria, se incluyan en la plataforma por lo que, en consecuencia, cabría la posibilidad de que la red social pudiera explotarlos económicamente. En todo caso, el consentimiento que presta el usuario debe entenderse otorgado desde el momento en que decide aceptar la política de privacidad y condiciones de uso de la plataforma. Debe advertirse que las políticas de privacidad deben ser transparentes, accesibles y claras.

Cuando se participe en la red como usuario y se publiciten contenidos que puedan representar riesgos significativos tanto para el propio titular como para terceros. Aunque sean los usuarios los que, de forma voluntaria, publican sus datos, los efectos sobre la privacidad pueden tener un alcance notablemente mayor al considerado inicialmente pues las plataformas en la que las redes sociales se fundamentan disponen de potentes herramientas de intercambio de información. En relación a los terceros[40], cabe indicar que los datos e imágenes que puedan, directa o indirectamente, afectarles deberán contar, con carácter previo, con su aquiescencia ya que en caso contrario estarán legitimados para reclamar su

[38] Los usuarios, antes de incluir los datos personales, deben valorar la modalidad concreta de los mismos pues no tiene, en absoluto, la misma trascendencia los datos personales de nivel básico –nombre, dirección, teléfono, etc.- que otros más sensibles –de carácter político, ideológico, religioso, sexual, etc.-. En consecuencia, tanto los usuarios como los responsables de las redes deben limitar y controlar, en todo momento, tanto el volumen como la importancia de los datos publicados en el perfil. Debe, en este sentido, considerarse que el art. 7 LOPD obliga a contar con un consentimiento expreso y por escrito respecto a los datos rela[tivos] a la ideología, religión y vida sexual. Sobre esta cuestión incide el documento de opinión 5/2009, de 12 de junio, emitido por el grupo de trabajo del Artículo 29 respecto a las redes sociales: 6 y 7.

[39] Tal aspecto es destacado por *Ofcom* (*Office of Communications*), en su estudio de abril de 2008 que tiene por rúbrica "Redes sociales: análisis cuantitativo y cualitativo sobre hábitos, usos y actuaciones". Para su consulta nos remitimos a www.ofcom.org.uk/advice/media.../socialnetworking/report.pdf.

[40] En relación a esta cuestión cabe destacar las manifestaciones realizadas por el Grupo de Trabajo del Artículo 29 en el documento de opinión 5/2009, de 12 de junio, respecto a las redes sociales en cuanto a que ciertas plataformas permiten, por medio de las etiquetas consignadas en las fotografías editadas por los usuarios registrados, identificar a terceros no miembros de las mismas lo cual constituye una actuación que puede vulnerar la privacidad.

retirada inmediata[41]. El Grupo Internacional sobre Protección de Datos en las Telecomunicaciones el pasado 4 de marzo de 2008 aprobó el *Rome Memorandum* en cuyo articulado se manifiesta que "uno de los desafíos que pueden observarse es que la mayoría de la información que se publica en las redes sociales se hace bajo la iniciativa de los usuarios y basado en su consentimiento". No debemos, a este respecto, olvidar que las redes sociales se fundamentan en el hecho de poner a disposición del público en general, la máxima cantidad posible de información personal del titular del perfil. Es por ello que, a efectos de privacidad, pueden plantearse complejas situaciones jurídicas que, han sido contempladas, en mayor o menor medida, por la propia legislación y, como complemento a ésta, por los códigos de conducta.

En el instante de darse de baja del portal ya que, a pesar de que la acción conducente a tal finalidad surtirá efectos, todo hay que decirlos, no serán plenos. En efecto, por un lado, durante cierto período de tiempo los motores de búsqueda de Internet[42], entre los que ocupa un lugar muy destacado el conocido *Google*, indexarán en sus búsquedas los perfiles de los usuarios –que, insistimos, pueden haber efectuado, con carácter previo, su baja efectiva de la red social en cuestión- junto con determinada información de contacto, imágenes así como perfiles vinculados de ese concreto individuo con otras personas. Por otro lado, cabe la posibilidad de que las redes sociales conserven los datos de tráfico[43] generados por los propios usuarios en el sistema para, posteriormente, emplearlos como

[41] La AEPD ha sancionado, en diferentes resoluciones –como, a título de ejemplo, es el procedimiento sancionador 00617/2008- la captación y publicación de imágenes de terceros en plataformas colaborativas sin consentimiento de las personas afectadas.

[42] Un buscador es una herramienta que facilita al usuario el acceso a determinados sitios *Web*. Para ello, la misma accede a una lista de enlaces previamente indexados y ofrece al usuario una relación de direcciones *Web* que remiten a páginas en las que figuran las palabras seleccionadas por el usuario. Debe ponerse de manifiesto que la legislación española incluye a los buscadores dentro de la definición de "servicios de la sociedad de la información" de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico. Así el apartado b) del Anexo define los servicios de intermediación como "el servicio de la sociedad de la información por el que se facilita la prestación o utilización de otros servicios de la sociedad de la información o el acceso a la información" y, añade, que son servicios de intermediación, entre otros, la provisión de instrumentos de búsqueda, acceso y recopilación de datos o de enlaces a otros sitios de Internet.

[43] Para ampliar está información nos remitimos a las interesantes consideraciones contenidas tanto en el Dictamen, de 4 de abril de 2008, sobre cuestiones de protección de datos en relación a los buscadores, realizado por parte del Grupo de Trabajo del Artículo 29 como a la Declaración sobre buscadores de Internet, de 1 de diciembre de 2007, en los que se analizan la conservación de datos de los usuarios por parte de los buscadores.

herramientas en virtud de las cuales podrán sectorizar y conocer las preferencias de los mismos para efectuar publicidad contextualizada.

En cuanto a los supuestos específicos de riesgo para la privacidad de los potenciales titulares de perfiles de redes sociales cabe referirse, sin ánimo agotador, a algunos de ellos. A continuación, enumeraremos tales peligros efectuando ciertas valoraciones a propósito de cada uno de ellos:

La recepción de correos electrónicos no solicitados o, en terminología anglosajona, *spam*[44]. Quienes, en los últimos años, vienen padeciendo, con cierta virulencia, está práctica son precisamente los usuarios de las redes sociales. Los avances que las redes sociales y las plataformas colaborativas suponen están modificando las prácticas comerciales[45], redefiniendo, de esta manera, la forma electrónica de ofertar bienes y servicios a través de la publicidad hipercontextualizada según los perfiles de usuario, diversificando el mercado y creando nuevos canales de comunicación. Los *spammers* pueden utilizar la información personal disponible en las redes sociales para recopilar direcciones de correo electrónico de modo que, cuando envíen *spam*, parezca que se envía desde los contactos directos[46]. En este sentido, debe precisarse que un correo electrónico recibido desde una dirección de un contacto, es mucho más probable que llegue a abrirse, pues parecerá, por decirlo en términos coloquiales, un correo "más fiable". Además, el *spammer* recogerá información relativa a aficiones o intereses con el fin de crear mensajes con temas de interés para el usuario, lo que, unido a que se recibe de un contacto, aumentará las posibilidades de que el usuario abra ese correo malicioso y que, en su caso, el *malware* que contenga, se active. En otras palabras, las redes sociales se han erigido en una poderosa herramienta de marketing para las empresas a la hora de promocionar sus productos y servicios ganando cada vez más terreno. Estos nuevos modelos de negocio basados en el comercio

[44] Como advierte SAMPOL PUCURRULL (2005): 1753-1760, el término *spam* o *spamming* tiene su origen en una práctica antigua en los países anglosajones en virtud de la cual se regalaba un jamón de escasa calidad –*spiced ham*- junto con las compras que se efectuaban en las carnicerías haciéndose, de esta forma, mención de un producto recibido sin ser, en principio, deseado.

[45] En este sentido, no resulta lícito el recurso a técnicas comerciales, como el *spam*, claramente vulneradoras de la privacidad. Así, a título de ejemplo, cabe referirse al caso en el que en 2008 una persona fue multada por un juez estadounidense a pagar más de 873 millones de dólares –unos 697 millones de euros- por mandar, a través de la red social *Facebook*, correos electrónicos no solicitados relativos a temas de orientación sexual, ofertas no solicitadas de medicamentos y otros productos. La imposición de la multa se efectuó en virtud de la Ley de Control de Pornografía y Marketing No Solicitados -*Controlling the Assault of Non-Solicited Pornography and Marketing Act*-. La sanción no cabe duda que tendrá un importante efecto disuasorio de cara a posibles infractores futuros de la norma mencionada.

[46] GONZÁLEZ DE LA GARZA (2008): 171.

electrónico pueden dar origen a un cierto grado de incertidumbre en el usuario sobre todo respecto a, entre otras cuestiones, la seguridad de las transacciones electrónicas, al perfeccionamiento y validez de los contratos o a la normativa aplicable o jurisdicción competente en caso de litigio.

Instalación y uso no permitido de técnicas electrónicas de monitorización del comportamiento. En este sentido, sin perjuicio de que existen otros muchos, cabe destacar dos instrumentos de notable relevancia en las redes sociales. Por un lado, el uso de *cookies* por parte de la plataforma que, durante la conexión a la misma, permitirá conocer ciertos datos del usuario que interactúe. Con tales herramientas técnicas puede conocerse, entre otros extremos, el lugar desde el que el usuario accede –fijo ó móvil-, el sistema operativo utilizado, los sitios más visitados, el número de *cliks* realizados, etc. Por otro lado, los *web bugs*, también denominados bichos o escuchas en la Red, "píxeles transparentes", "*web beacons*", "*pixel gif*" o "*web pings*" tienen que ver con actuaciones inconscientes cuya repercusión podría pasar desapercibidas. En efecto, para registrar y rastrear la apertura de un documento –por ejemplo, un correo electrónico- por Internet, se incluye en el mismo una imagen vinculada a un servidor distinto al que aloja la página que estamos visitando. Son gráficos de un píxel por un píxel que instalan un programa en el disco duro con la finalidad de leer todas las *cookies* incluidas en el mismo. Cuando se abra la página se pedirá al servidor ese archivo y quedará registrada la IP del solicitante. El hecho de solicitar la imagen vinculada permitirá recabar, entre otras cuestiones, la dirección IP del ordenador, la fecha y hora en que se visitó la página donde estaba insertada la imagen, el tipo y versión de navegador del consumidor o usuario, su sistema operativo, el idioma predeterminado o los valores de *cookies*. De esta manera, se recogen numerosos datos estadísticos y se consigue efectuar el seguimiento de los usuarios. Impedir el uso de los dispositivos enunciados o, al menos, que se haga dentro de ciertos límites que garanticen, en todo caso, el respeto de la privacidad viene siendo, en los últimos años, una prioridad de la UE y, evidentemente, de España. La Directiva 2002/58/CE se ha ocupado de los mismos considerando, a título de ejemplo, que las *cookies* es una técnica lícita siempre y cuando se informe al titular de los datos de ello y, a su vez, se obtenga su consentimiento así como que la utilización de tal práctica responda a un fin legítimo. De este modo, parece que, a nivel comunitario, se permite el uso de las *cookies* cuando previamente haya sido advertido. Debe destacarse la existencia de una Propuesta de Directiva del Parlamento y del Consejo, de 13 de noviembre de 2007, que, entre otras modificaciones, pretende dar una nueva redacción a diversos pre-

ceptos de la citada Directiva 2002/58/CE (más conocida como Directiva sobre la privacidad y las comunicaciones electrónicas), entre otros, al artículo 5.3[47] donde se establecerá la prohibición del uso de programas espía y de otros programas informáticos maliciosos en el marco del Derecho comunitario, independientemente del método utilizado para su entrega e instalación en los equipos de los usuarios –distribución a través de descargas de Internet o de medios externos de almacenamiento de datos, como CD-ROM, llaves USB, etc.-.

Ser víctima de prácticas manifiestamente delictivas como el *phishing*[48] y *pharming*[49]. Por paradójico que pueda resultar es frecuente que los usuarios utilicen la misma contraseña de acceso, en su participación como miembros de diversas comunidades virtuales, lo que supone que si en cualquiera de ellas existiera un fallo de seguridad las consecuencias de tal hecho podrían extenderse a los demás portales pues con la misma contraseña podría accederse a todos los portales. La delicada situación que planteamos se agrava, aun más si cabe, cuando los usuarios tienen la misma contraseña para efectuar operaciones financieras[50].

La indexación de perfiles, en todo caso no permitida, por parte de buscadores electrónicos[51]. En numerosas ocasiones, las redes sociales posibilitan que los motores de búsqueda indexen en sus exploraciones los

[47] El actual artículo 5.3 de la Directiva sobre intimidad y comunicaciones electrónicas aborda la cuestión de las tecnologías que permiten recopilar información u obtener acceso a la información ya almacenada en el terminal de un abonado o usuario únicamente por medio de la red de comunicaciones electrónicas.

[48] Estamos ante un tipo de estafa que intenta obtener información personal –en especial de acceso a servicios financieros- mediante la suplantación de la apariencia o el nombre de una determinada entidad bancaria. Como bien advierten RODRÍGUEZ LÓPEZ DE LEMUS y BORREGO ZABALA (2008): 92 y 93, nos encontramos ante un fenómeno que suele difundirse a través de *spam*.

[49] El *pharming* es una técnica que redirige desde la página *Web* solicitada por el usuario a otra predeterminada por el atacante con la finalidad de hacerle creer que se encuentra en la deseada y actúe dentro de la misma con total normalidad. El *pharming* se diferencia del *phishing* en que el segundo nos invita a acceder a una página *Web* o proporcionar datos, a través de un correo electrónico que ha entrado en nuestro buzón. En el *pharming*, el código malicioso que opera se puede haberse introducido en nuestro ordenador por cualquier medio y, sin que nos hayamos percatado de ello, reconfigura el *software* que tenemos instalado alterando la relación entre el número IP y la dirección de Internet que escribimos en el ordenador.

[50] En este sentido, pone de relieve el INTECO (2009): 25 que algunas de las redes sociales electrónicas más representativas han sido objeto de ciertos fraudes electrónicos. En efecto, se han producido situaciones en las que una persona se hace pasar bien por un conocido en quien confía bien por una reputada empresa que opere en esa plataforma electrónica para, de este modo, conseguir cierta información personal así como claves bancarias.

[51] Debe tenerse en consideración, por la importancia que a nuestros efectos representa, el mencionado Dictamen, de 4 de abril de 2008, sobre cuestiones de protección de datos en relación a los buscadores, realizado por parte del Grupo de Trabajo del Artículo 29 cuyo objetivo es "es lograr un

perfiles de los usuarios[52], junto con información personal y otros contactos vinculados lo que supone un importante riesgo para la privacidad[53] además de, naturalmente, dificultar el proceso de eliminación de su información en Internet.

Violaciones de identidad. Un fenómeno relativamente en la actualidad viene determinado por el hecho de la suplantación de identidad de determinados usuarios que, sin haberse registrado con carácter previo en la plataforma, cuando van a registrarse en la misma pueden llevarse la desagradable sorpresa de que su identidad digital ya existía mucho antes en la red social.

4. Especial consideración de los menores de edad e incapaces

A nivel nacional, existe una normativa que tutela el colectivo de los menores de edad e incapacidad por lo que a la privacidad respecta. Como seguidamente veremos, tenemos ante sí una materia que, desde hace ya aproximadamente una década, fue abordada en una de sus memorias anuales –del año 2000- por parte de la Agencia Española de Protección de Datos (AEPD). Seguidamente, se hicieron eco de la misma, por lo que al ámbito electrónico respecta, los códigos de conducta, deontológicos o de buena práctica en materia de comercio electrónico[54] que, con buen criterio, fueron asumidos –y, a fecha de hoy, tal corriente continúa- por un número nada desdeñable de prestadores de servicios de la sociedad de la información. Posteriormente, el Reglamento de desarrollo de la Ley Orgánica de Protección de Datos de carácter Personal –aprobado por Real Decreto 1720/2007 de 21 de diciembre- incorporó en su articulado las prescripciones legales que han de observarse para poder recabar

equilibrio entre las necesidades empresariales legítimas de los proveedores de los buscadores y la protección de los datos personales de los usuarios de Internet".

[52] Consciente de los problemas que venimos comentando el Grupo internacional sobre protección de datos en las telecomunicaciones adoptó, ya hace más de una década, una posición común sobre protección de la intimidad y buscadores el 15 de abril de 1998, revisada el 6-7 de abril de 2006. El Grupo de Trabajo compartió en esta última sus preocupaciones sobre el potencial de los buscadores de permitir la creación de perfiles de personas físicas.

[53] Sobre este particular, debemos advertir que la Agencia Española de Protección de Datos, en diferentes resoluciones –como, entre otras muchas, la 01046/2007 de 20 de noviembre de 2007- ha tutelado el derecho de oposición del que el usuario goza respecto a la indexación del nombre u otro tipo de datos de carácter personal en los buscadores ya que tal actuación constituye un tratamiento automatizado de datos que debe adaptarse a la normativa legal vigente.

[54] En este sentido, AENOR, Agace, Agencia de Calidad de Internet, E-Confía, E-Web y Óptima Web.

el consentimiento de los menores de edad a efectos de tratamiento de sus datos de carácter personal.

De la memoria anual de la AEPD del año 2000 así como de las consideraciones presentes en los códigos de conducta de comercio electrónico parece, como acabamos de manifestar, haberse hecho eco el art. 13 Reglamento de desarrollo de la LOPD. Y es que, como se deduce de la lectura del precepto apuntado, debemos distinguir dos grandes grupos, con una regulación, en lo que a la manera de recabar el consentimiento respecta, diversa dentro del colectivo de los menores de edad. Por un lado, aquellos mayores de 14 años de edad que, por sí solos, podrán prestar su consentimiento, para el tratamiento de sus datos personales, salvo en los supuestos en los que, por imperativo legal, tal consentimiento precise la asistencia de los representantes legales. Por otro, los menores de 14 años para cuyo tratamiento de datos personales será preceptivo, como regla general, el consentimiento de sus progenitores o tutores.

Asimismo, se establece la prohibición de explotar la incredulidad y especial vulnerabilidad de los menores de edad –dentro de los que deben considerarse incluidos a todos los que todavía no han adquirido la mayoría de edad- para obtener información, de diversa índole, sobre la unidad familiar como, por ejemplo, son sus características profesionales, económicas, sociológicas u otras para cuyo efectivo conocimiento será preceptivo el previo consentimiento de sus titulares.

En el caso de que pretendan tratarse datos de menores de edad el lenguaje empleado para recabar tal consentimiento –aplicable únicamente para los mayores de 14 años pues para los menores de tal edad será preciso el consentimiento exclusivo de sus representantes legales- deberá ser claro y suficientemente comprensible para un menor con indicación expresa de lo dispuesto en el art. 13 Reglamento desarrollo LOPD. Tal exigencia implica el empleo de una terminología sencilla dentro del que debe entenderse incluida la imposibilidad de recurrir a tecnicismos, términos ambiguos o expresiones cuya efectiva comprensión sea ardua para un menor. Naturalmente, no será igual la comprensión y vocabulario que podríamos considerar inteligible para un menor con 14 años que para un menor que está próximo a la mayoría de edad. En cualquier caso, atendiendo al espíritu del precepto, debemos considerar que la intención del legislador ha sido no hacer distingos, en este sentido, por lo que se refiere a la madurez exigible al menor a lo largo de su evolución natural. Es por ello que entendemos que el lenguaje empleado para recabar la autorización, para consentir el tratamiento de los datos personales del menor de edad, deberá ser lo suficientemente claro y sencillo para que pueda

ser perfectamente comprensible tanto por un mayor de 14 años recién cumplidos como por un menor a punto de adquirir la mayoría de edad.

El responsable del fichero será el encargado de asegurar la efectividad del procedimiento mediante el que se recabe el consentimiento del menor en el caso de que sea mayor de 14 años[55]. En el supuesto de que sea menor de 14 años así cuando la Ley así lo disponga para los mayores de 14 años deberá garantizarse la autenticidad del consentimiento prestado por los representantes legales.

En todo caso, las propias redes sociales tienen la obligación de disponer de medios tecnológicos que garanticen la identificación de edad de los usuarios. Nos encontramos ante una cuestión realmente importante que, con relativa frecuencia, se plantea en la práctica. De hecho, en este sentido, la AEPD ha tenido la ocasión de condenar, en diferentes procedimientos sancionadores[56], la falta de diligencia en la comprobación de la identificación de un menor que se registró en un determinado sitio *Web* siendo sus datos empleados para remitirle publicidad.

Las disposiciones legales aprobadas en España para asegurar la protección de la privacidad de los menores de edad son exigibles sólo a escala nacional. *A sensu contrario*, la aplicación de la normativa española no podrá exigirse ni en el espacio comunitario ni el internacional pues no debe olvidarse que la ley únicamente desplegará eficacia en el espacio territorial. Uno de los mayores obstáculos que precisamente se presentan para conseguir una efectiva garantía y tutela de la privacidad es la falta de instrumentos jurídicos que afirmen la extraterritorialidad de las conductas ilícitas de tratamiento informatizado de la información en relación con las que el territorio físico no tiene trascendencia alguna. Esta última precisión es especialmente relevante en el ámbito de las redes sociales. En todo caso, Tuenti, al ser española, está sometida a la actual legislación en materia de protección de datos y, por tanto, como se deduce de su actual política de privacidad, ofrece mayores garantías de que la información

[55] ALMUZARA ALMAIDA, COUDERT, MARZO PORTERA y NAVALPOTRO NAVALPOTRO, (2008): 38 y 39; DEL PESO NAVARRO, RAMOS GONZÁLEZ, DEL PESO RUIZ y DEL PESO RUIZ (2008): 66 y 67.

[56] Así, entre otros muchos, el procedimiento sancionador 00281/2007 en el que se sanciona a las entidades incumplidoras –Antevenio, por un lado, y Bankinter, por otro- con cuantiosas multas pecuniarias. A Antevenio se le sanciona, por una infracción de los artículos 6.1 y 11.1 de la LOPD, tipificadas como grave y muy grave en los artículos 44.3.d) y 44.4.b) de dicha norma, respectivamente, una multa de 60.000 € y una multa de 150.000 €, de conformidad con lo establecido en el artículo 45.2, 3, 4 y 5 de la citada Ley Orgánica. A Bankinter se le impone, por una infracción del artículo 6.1 de la LOPD, tipificada como grave en el artículo 44.3.d) de dicha norma, una multa de 60.000 €, de conformidad con lo establecido en el artículo 45.2, 4 y 5 de la citada Ley Orgánica.

personal queda sujeta a las normas de seguridad legalmente imperantes. Pero, la inmensa mayoría de redes sociales están al margen de la ley española e, incluso, de la europea.

Para, precisamente, incrementar el nivel de seguridad de las redes sociales, con respecto a los menores de edad, la Comisión Europea, el pasado 10 de febrero de 2009, intervino en un acuerdo entre los principales prestadores de tales servicios[57] denominado *Safer Social Networking Principles for the UE*. Iniciativas como las que comentamos unifican criterios y consiguen una protección más homogénea para los usuarios de las redes sociales. Tal compromiso, que representa una interesante manifestación de la autorregulación del sector[58] (de la que seguidamente nos ocuparemos), que carece de fuerza jurídica vinculante por lo que no deja de ser una simple declaración de intenciones, ha sido suscrito para, entre otros factores, mejorar la privacidad de los menores de edad. Las medidas[59] que, en virtud de tal acuerdo, se pondrán en práctica tienen como fin alcanzar, para los menores de edad en el ámbito de las redes sociales, una protección de mayor nivel que la que podría alcanzarse por la legislación.

[57] Se trata de las siguientes: *Arto*, *Bebo*, *Dailymotion*, *Facebook*, *Giovani.it*, *Google/YouTube*, *Hyves*, *Microsoft Europe*, *Myspace*, *Nasza-klaza.pl*, *Netlog*, *One.lt*, *Skyrock*, *StudiVZ*, *Sulake/Habbo Hotel*, *Yahoo!Europe* y *Zap.lu*.

[58] Los acuerdos suscritos entre los distintos prestadores de servicios de redes sociales y los poderes públicos –de diferente alcance según el espacio territorial en el que estos últimos se encuentren radicados- no se reducen al espacio europeo (que, dicho sea de paso, será nuestro objeto de estudio) sino que también se han operado en el espacio norteamericano. En este sentido, cabe aludir al convenio alcanzado entre *Facebook* y *MySpace* con 49 fiscales generales en los Estados Unidos con la finalidad de garantizar la protección integral de la privacidad de los menores de edad.

[59] Las actuaciones acordadas por los prestadores para implementar un elevado nivel de protección de los menores de edad en las redes sociales son: 1. proporcionar un botón de denuncia de abusos, fácil de utilizar y accesible, que permita a los usuarios manifestar, con un solo *clic*, contactos o comportamientos inadecuados de otros usuarios; 2. asegurarse de que todos los perfiles y listas de contactos en línea de los usuarios de los sitios *Web* registrados como menores de 18 años estén predeterminados como privados, en el sentido, de que su contenido no sea visible para terceros; 3. cerciorarse de que los perfiles privados de los usuarios menores de 18 años no puedan buscarse ni en los sitios *Web* ni a través de motores de búsqueda; 4. garantizar que las opciones de privacidad estén destacadas y sean accesibles en todo momento, de manera que los usuarios puedan averiguar fácilmente quién puede ver lo que editan en sus perfiles y; 5. impedir que los menores de edad de menos de 13 años utilicen sus servicios. Si una red social está dirigida a adolescentes de más de 13 años, a los menores de esa edad debe resultarles difícil registrarse. A tal efecto, deberán arbitrase las medidas técnicas oportunas.

IV. LA AUTORREGULACIÓN COMO ESTRATEGIA ORDENADORA IDÓNEA DE LAS ACTIVIDADES QUE SE DESARROLLAN EN LA RED

1. Consideraciones previas

La autorregulación en general y los códigos de conducta en particular constituyen una materia huérfana de estudio desde el punto de vista jurídico. Representa una cuestión de la que, todo hay que decirlo, apenas se ha ocupado tanto la doctrina como la propia jurisprudencia a pesar de que el legislador, como seguidamente veremos, recurre a la misma para, precisamente, fomentar y, posteriormente, consolidar su vigencia en diversos ámbitos cual, en nuestro caso, son tanto el comercio electrónico como las redes sociales.

Debe ponerse de manifiesto que la autorregulación es una figura encarecidamente sugerida por el legislador, comunitario[60], estatal[61] y autonómico[62], en diferentes textos normativos. Uno de los ámbitos en los que se aspira a conseguir la vigencia plena y efectiva de la fórmula reguladora que analizamos es, como seguidamente veremos, en el comercio electrónico y en las redes sociales.

La autorregulación, como determina el Diccionario de la Real Academia de la Lengua Española de 2006, es la acción y el efecto de autorregularse, siendo éste último vocablo el hecho de regularse por sí mismo. Dicho de otra forma, tal opción pasa por la ordenación de una deter-

[60] Así, entre otras, cabe poner de relieve la Directiva 97/7/CE, de 20 de mayo de 1997, relativa a la protección de los consumidores en materia de contratos a distancia; Decisión 276/1999/CE del Parlamento Europeo y del Consejo, de 25 de enero de 1999, por la que se aprueba un plan plurianual de acción comunitaria para propiciar una mayor seguridad en la utilización de Internet mediante la lucha contra los contenidos ilícitos y nocivos en las redes mundiales; Directiva 2000/31/CE, de 8 de junio, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior; Directiva 2005/29/CE, de 11 de mayo de 2005, relativa a las prácticas comerciales desleales de las empresas en sus relaciones con los consumidores en el mercado interior; Directiva 2006/123/CE, de 12 de diciembre, relativa a los servicios en el mercado interior; Resolución del Parlamento Europeo, de 21 de junio de 2007, sobre la confianza de los consumidores en un entorno digital; y las Conclusiones del Consejo, de 22 de mayo de 2008, sobre un planteamiento europeo de la alfabetización mediática en el entorno digital.

[61] Procede destacar, entre otras, la Ley 7/1996, de 15 de enero, de Ordenación del Comercio Minorista; y la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico.

[62] Cabe referirse, a título de ejemplo, al Decreto de Castilla La Mancha 101/1996, de 25 de julio, que regula el Consejo Regional de Consumo; Ley de la Comunidad de Madrid 11/1998, de 9 de julio, sobre Normas Reguladoras de Protección al Consumidor; Ley 3/2003, de 12 de febrero, del Estatuto de los Consumidores y Usuarios de la Comunidad Autónoma de Canarias; y Ley 13/2003, de 17 de diciembre, de Defensa y Protección de los Consumidores y Usuarios de Andalucía.

minada materia –en nuestro caso de las redes sociales- por parte de los agentes que interactúan en la misma.

Las ventajas del sistema de autorregulación, entre otras, son: voluntariedad, lo que facilita considerablemente su aplicación práctica y su cumplimiento sin necesidad de intervención e imposición de los poderes públicos; flexibilidad; especialización; favorecer el desarrollo de estándares que garantizan elevados niveles de corrección; transparencia; prevención de infracciones, en el ámbito reglamentado, sobre todo si se dispone de mecanismos de valoración previa; bajo coste en diferentes ámbitos cual, por ejemplo, es en los procedimientos por infracciones; el hecho de cubrir eventuales lagunas de carácter legal; y fácil acceso. Por último, aunque no por ello menos relevante, es preciso tener en cuenta las ventajas de ahorro de tiempo y de recursos jurídicos y económicos para los poderes públicos que puede conllevar la potenciación de estas técnicas de autorregulación en los diferentes modelos de protección al potencial consumidor y/o usuario. Y ello porque, además de este plus de protección en que se traducen todas estas técnicas para el consumidor, puede ayudar a liberar al propio sistema jurídico-público de los costes de la regulación. En definitiva, la presencia de tales prerrogativas hace del mismo un sistema verdaderamente eficaz y aconsejable en el ámbito de las redes sociales[63].

La fórmula que disciplina las relaciones sociales acontecidas en un determinado sector, cual es la autodisciplina, siempre ha existido, de una u otra manera, pues, naturalmente, cualquier organización, de algún modo, se autorregula. El fenómeno de la autorregulación supone la observancia de unas pautas de conducta –principios y normas éticas- cuyo cumplimiento previamente se ha fijado como objetivo. Simultáneamente, también constituye la expresión del compromiso de responsabilidad social de un determinado sector de la industria.

En base a que la autorregulación es una práctica más informal que la legislación y que carece de capacidad coactiva –entendida ésta en el sentido de una virtualidad y alcance cercano a la estatal-, la eficacia de la misma puede ser muy débil si no se da un entorno cultural favorable y la organización de todas las partes implicadas. Hay que observar, asimismo, que la autorregulación no puede ser vista como una excusa que exima al

[63] SIRINELLI (1998): 1-22; EDELSTEIN (2003): 509-543; FELIU ÁLVAREZ DE SOTOMAYOR (2006).

poder legislativo de sus obligaciones, sino como complemento[64] a una legislación que, inevitablemente, no puede dejar de tener un carácter ciertamente general y ambiguo. Podemos, de esta manera, afirmar, en cierto sentido, que la profesionalización del sector empresarial conduce a su autorregulación[65]. La presión reguladora de los poderes públicos, tendente a fomentar e, incluso, a imponer, en ciertos casos, la autorregulación, no es sino una manifestación de la necesidad de aumentar el grado de profesionalización de las empresas[66].

La autorregulación jurídicamente relevante es aquella que resulta inteligible y aceptable por el sistema del Derecho llegando, en ciertos supuestos, a incorporarla como si de una referencia propia se tratara. En el seno de semejante consideración debemos entender incluida la previsión del legislador de promocionar la autorregulación en sectores de elevada complejidad técnica cual son tanto el comercio electrónico como las redes sociales.

2. Situación imperante en materia de comercio electrónico

En los últimos años, somos testigos y, en ciertos casos, protagonistas de un vigoroso impulso, fomentado desde diversas instancias, del *soft law*[67] –en terminología anglosajona- o derecho no vinculante especialmente por lo que respecta a la protección de los consumidores y/o usuarios en Internet en general y en materia de comercio electrónico en particular. El derecho no vinculante o voluntario es el conjunto de instrumentos que, aunque no ostentan el carácter imperativo que caracterizan a las normas jurídicas, pueden afectar, de manera significativa, al panorama legislativo promoviendo la estandarización legal de determi-

[64] En este sentido, CHISSICK y KELMAN (2002): 67; PUNZÓN MORALEDA y SÁNCHEZ RODRÍGUEZ (2004): 63-78; BENNET y RAAB (2006): 151-159.

[65] CAMPUZANO TOMÉ (2000); VELÁZQUEZ BAUTISTA (2001).

[66] La autodisciplina en el ámbito de las redes sociales debe ser una labor que implique a todos los agentes sociales. En este sentido, el director de la AEPD insistió, en la comparecencia del mes de junio del 2009 ante la Comisión Constitucional del Congreso de los Diputados, en la recomendación a los medios de comunicación para que alcancen un desarrollo de buenas prácticas en materia de privacidad, a través de la autorregulación, en relación a la difusión de informaciones privadas de menores obtenidas de redes sociales, cuando son objeto de interés informativo (caso, por ejemplo, de la publicación de imágenes de Marta del Castillo).

[67] Sobre las diferencias que existen entre las normas jurídicas o *hard law* y las normas de carácter deontológico o *soft law* nos remitimos a las consideraciones de, entre otros autores, PAZ-ARES RODRÍGUEZ (2000): 85-98; SHAPIRO (2002): 15-32.

nadas prácticas[68]. Debe ponerse de manifiesto que la falta de fuerza vinculante del derecho no vinculante no implica la carencia total de efectos jurídicos. En efecto, las prácticas susceptibles de ser englobadas en aquél se erigen en un modelo de referencia sugerido, como ya hemos visto, por parte de instancias públicas.

Es conveniente, en este sentido, poner de manifiesto que los códigos de conducta no pueden establecer normas cuya aplicación sea más permisiva que el mínimo exigido por la ley ni tampoco, naturalmente, ser abiertamente contrarios a la ley imperativa. Naturalmente, no es admisible una rebaja de la normativa legal fijada por parte del legislador, como ley imperativa o, en su caso, semiimperativa –a favor del consumidor-. Sí que realizan, no obstante, una importante mejora del marco tuitivo aplicable al potencial consumidor y/u usuario –parte débil del contrato- en materia de comercio electrónico.

La autorregulación del comercio electrónico y, consecuentemente, su instrumento más paradigmático a efectos de confianza, el código de conducta, es posible en virtud del principio de la autonomía de la voluntad. Tal principio es objeto de disciplina por el art. 1255 Código civil que, como es sabido, establece que "los contratantes pueden establecer los pactos, cláusulas y condiciones que tengan por conveniente, siempre que no sean contrarios a las leyes, a la moral, ni al orden público".

Los códigos de conducta en materia de comercio electrónico pueden ser definidos como documentos, de carácter voluntario, que incluyen un conjunto de principios, reglas o, en definitiva, buenas prácticas, certificables por una tercera parte independiente, en cuya redacción se han tenido en consideración los intereses de asociaciones de consumidores y usuarios, discapacitados[69] u otros colectivos afectados, que disciplinan materias relativas al procedimiento precontractual, contractual y postcontractual por lo que a la contratación electrónica respecta, sin perjuicio de otras cuestiones como la publicidad interactiva, la seguridad, la privacidad, la accesibilidad y la protección integral de los menores de edad amén de otras conexas, cuya finalidad es la instauración y consolidación de la confianza del potencial consumidor y usuario.

[68] ESPINOSA CALABUIG (2001); ARRANZ ALONSO (2003): 197-269; PATIÑO ALVES (2007).

[69] La previa toma en consideración de diferentes colectivos para la redacción de los códigos de conducta no ha merecido la misma acogida por parte de la doctrina. Así, en opinión de ciertos autores – GÓMEZ CASTALLO (2001): 133-146; RUIZ NÚÑEZ (2003): 295-307-, ha de valorarse positivamente mientras que, por el contrario, a juicio de otros –VÁZQUEZ IRUZUBIETA (2002)- tal postulado merece una valoración reprobable.

Las normas que se recogen en estos códigos suelen estar mucho más adaptadas al problema concreto que quieren solucionar ya que la elaboración de los mismos se ha efectuado, precisamente, por las personas que se encuentran en una relación más cercana con la problemática a resolver[70].

La Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI-CE) justifica el recurso a los códigos de conducta, sobre la temática antes enunciada, en virtud de su utilidad como instrumento de autorregulación especialmente apto para adaptar el articulado de la ley a las características específicas de cada sector. Es por ello que, conocedor de las particularidades que los códigos de conducta representan, determina que corresponde al sector público promover, mediante la coordinación y el asesoramiento, la creación y aplicación de tales instrumentos.

Debemos mencionar, por la relevancia que ostenta a nuestros efectos, la existencia del código de conducta europeo de la Federación Europea de comercialización directa sobre utilización de datos personales en la comercialización directa cuyo contenido se ajusta a la Directiva 95/46/CE de privacidad, proporcionando el suficiente valor añadido a dicha Directiva ya que está adecuadamente centrado en las cuestiones y problemas específicos de la protección de datos en el sector de la comercialización directa y ofrece soluciones suficientemente claras para dichas cuestiones y problemas.

Las empresas que se adhieran al sistema de autorregulación deben poder mostrar a sus eventuales clientes que pertenecen al mismo, de forma que el consumidor conozca el sistema de protección de los derechos e intereses del usuario que se pone a su servicio. Es preciso, por consiguiente, que exista un mecanismo de acreditación de la adhesión al sistema de autodisciplina, de forma que sean identificadas las empresas comprometidas activamente con su sostenimiento y desarrollo. Tal extremo, se pondrá de manifiesto mediante la exhibición en un lugar visible de la página *Web*, por parte de la empresa signataria del código de conducta en cuestión, del correspondiente sello de confianza acreditativo de la adhesión de la empresa a aquél[71].

[70] BENNET y RAAB (2006): 151-158.

[71] KUHLMANN (1990): 28; BOCK (2000): 39; GIERL y WINKLER (2000): 197-207; RUSSELL y LANE (2002): 112; KROEBER-RIEL y WEINBERG (2003): 68.

En cuanto al posible contenido que los códigos de conducta podrán presentar en materia de comercio electrónico cabe insistir en el hecho de que podrán contener bien una regulación integral del comercio electrónico, incluyendo las cuestiones relativas a la privacidad, bien estar dedicados, por completo, a la ordenación de la protección de datos en aquél ámbito. En cualquier caso, el código ético contendrá –con más o menos detalle- medidas dirigidas a garantizar la protección de datos de carácter personal tanto de los mayores de edad como de los menores de edad[72].

Uno de los códigos de conducta que supone un verdadero referente empresarial en los ámbitos descritos es el de la Agencia de Calidad de Internet[73]. Esta última, que constituye una asociación sin ánimo de lucro surgida de la fusión de los dos sistemas de autorregulación en materia de comercio electrónico que hasta la fecha eran los más representativos a nivel nacional -Iqua y Confianza Online-, la componen, además de Red.es -Ministerio de Industria-, los Consejos Audiovisuales de Cataluña, Andalucía, Navarra y Andorra, Autocontrol y AECEM. Como puede apreciarse, nos encontramos ante una asociación fundada por 7 entidades, 2 de ellas privadas: AECEM y Autocontrol, representando a la industria publicitaria (anunciantes, agencias y medios); y 5 públicas: Consejos Audiovisuales de Andalucía, Andorra, Cataluña y Navarra y el Ministerio de Industria, Comercio y Turismo a través de la entidad pública empresarial Red.es.

El título 4 del mencionado código ético contiene uno de los núcleos centrales de los códigos de conducta que no es otro que la privacidad dedicando siete artículos a su análisis. La protección de datos personales representa un área de indudable y necesario interés, por ser merecedora de una adecuada salvaguarda en el desarrollo de actividades, tanto en el ámbito de la publicidad interactiva como en el del comercio electrónico.

[72] Por lo que a la protección de la privacidad en Internet de los menores de edad debemos citar como referente internacional en la materia pues marcó un hito, dado tanto el momento de su aprobación como su contenido, la regulación norteamericana denominada *Children´s Online Privacy Protection Act* –COPPA- de 21 de octubre de 1998 cuya entrada en vigor tuvo lugar el 21 de abril de 2000. Tal regulación versa sobre el control de la información personal de menores de 13 años de edad recopilada a través de Internet y cómo luego se utiliza dicha información.

[73] Respecto al examen íntegro de la mencionada asociación recomendamos la lectura de LÓPEZ JIMÉNEZ (2009a): 10-14 y LÓPEZ JIMÉNEZ (2009b): 9-14.

3. Escenario vigente y perspectivas de futuro por lo que a las redes sociales se refiere

Por todo cuanto hasta el momento hemos visto puede tomarse conciencia, como consecuencia de los eventuales perjuicios que eventualmente podrían derivarse, de la imperiosa necesidad de garantizar elevados niveles de protección de la privacidad en el ámbito de las redes sociales. Aunque nos encontramos ante plataformas inexcusablemente sometidas a la legislación que en materia de protección de datos personales impera, no cabe perder de vista que las leyes son, por naturaleza, limitadas, desde su origen, pues, como regla general, sólo despliegan eficacia en el espacio territorial para el que precisamente han sido concebidas[74]. En Internet, como es sabido, no existen fronteras territoriales y, si bien las leyes nacionales son aplicables, la virtualidad, que, en la práctica, despliegan es extraordinariamente limitada.

Como consecuencia de las valoraciones previamente esgrimidas se hace, de todo punto, conveniente, como ya se ha sugerido desde instancias comunitarias, fomentar, en primer término, la creación de un código de conducta regulador de las redes sociales cuyo alcance será, inicialmente, el espacio comunitario si bien lo deseable, todo hay que decirlo, hubiera sido un código de conducta de alcance internacional. En todo caso, no debe infravalorarse la importancia del paso dado pues tal decisión no representa, en modo alguno, óbice para que, en el futuro, se alcance un código de conducta internacional.

En la actualidad, no se ha elaborado código de conducta alguno, en el espacio comunitario, si bien, como en varias ocasiones hemos determinado, presumiblemente tendrá lugar próximamente –segundo semestre de 2009 o primero de 2010-. No debe olvidarse que tal código de conducta será de carácter, en todo caso, voluntario. En efecto, su articulado se erigirá en un referente en materia de protección de datos en el ámbito de las redes sociales no siendo, en consecuencia, obligatorio, si no ha sido previamente asumido, para las plataformas. Las redes sociales que deseen adherirse al mismo, con tal actitud, pondrán de manifiesto, de manera pública, que su comportamiento, desde el punto de vista de la protección de la privacidad de los usuarios, es más tuitivo para el usuario que lo que al respecto determina la propia legislación. En otras palabras, en ciertos supuestos, se mejorarán las disposiciones legales a favor del usuario mientras que, en otros, se cubrirán eventuales vacíos legales. Debe

[74] PIÑAR MAÑAS (2008b): 91.

valorarse, en este sentido, que nos encontramos ante un entorno tan dinámico que las leyes nacionales no son capaces de regular con cierta premura debido, fundamentalmente, a la rapidez con la que se suceden los cambios, de diferente índole, en la sociedad de la información y del conocimiento. En cualquier caso, no nos encontramos ante un problema nuevo ya que, tradicionalmente, la legislación ha resuelto problemas de aplicación de las tecnologías, aunque con cierto retraso, según éstas han ido suscitando nuevas dificultades al cuerpo doctrinal legislativo. Tal inconveniente, inherente al propio procedimiento de elaboración de las normas, podría eludirse (o, al menos, relativizarse) de acudirse a la figura de los códigos de conducta reguladores de las redes sociales pues tales normas, de origen convencional, fruto de la autorregulación, tienen un período de elaboración notablemente más corto y menos formalista que las normas legales siendo, dicho sea de paso, su capacidad de adaptación a los cambios tecnológicos notablemente mayor.

En cuanto a las cuestiones que, a nuestro criterio, deberían abordarse en tal documento, revelador de las mejores prácticas por lo que a la privacidad se refiere en el ámbito de las redes sociales, pondremos de manifiesto algunas de ellas sin que, en absoluto, pueda entenderse como agotadoras de las realmente posibles. Nótese, por consiguiente, que cuanto apuntaremos únicamente es un mínimo ejemplo de contenidos. Haremos, en este sentido, mención de la necesidad de insistir en cuestiones de fondo y de forma.

Respecto a las últimas es fundamental que el articulado del código deontológico establezca la obligación de que las redes sociales expongan toda la información relativa a sus servicios de manera clara y sencilla. El lenguaje empleado en sus políticas de privacidad debería ser comprensible por cualquier usuario permitiéndole conocer sus derechos y obligaciones.

Uno de los contenidos más plausibles de los códigos de conducta debería venir, precisamente, determinado por la necesidad de promocionar, por parte de los diversos agentes que suscriben su contenido, una campaña, a través de diferentes medios, de información y educación por lo que se refiere a las materias reglamentadas. A este respecto, cabe señalar que, en octubre de 2007, la *European Network and Information Security Agency* –ENISA- hizo público un estudio rubricado "Recomendaciones y seguridad para las redes sociales online". En tal documento, se efectúan un amplio catálogo de recomendaciones –dirigidas tanto a los propios proveedores de redes sociales como a los órganos encargados de aprobar la normativa que en cada caso proceda- entre los que, a nuestros

efectos destaca, la necesidad de invertir en la educación de los usuarios de estas redes. En suma, el fomento de códigos de buenas prácticas de las comunidades de una red social puede contribuir, de forma importante, a la formación y concienciación de los usuarios. Sería deseable, en este sentido, fijar la necesidad de que las redes sociales instauren, en sus respectivas páginas de inicio, un apartado específico dirigido a informar a los usuarios de las condiciones del servicio y de los efectos de cada una de las acciones que, en su caso, realicen.

A nivel técnico, debería arbitrarse la obligación de implantar ciertas acciones como, entre otras, son: establecer aplicaciones de seguridad dirigidas a garantizar o, en su caso, mitigar la posibilidad de recibir mensajes comerciales no deseados a través de la red social; instaurar medidas tecnológicas que permitan conocer la edad de los usuarios lo cual es especialmente importante a efectos de limitar la entrada de los menores de edad; constituir herramientas dirigidas a reducir los casos de suplantación de identidad por parte de los usuarios dentro de la red; eliminar los datos obsoletos que pudieran existir en distintos servidores así como el cifrado de aquellos que estén en uso minimizándose, de este modo, los perjuicios que pudieran derivarse de un ataque desde el exterior por parte de terceros malintencionados; crear mecanismos de análisis respecto de la fortaleza de la contraseña de forma que únicamente se admita aquella que sea suficientemente segura para el usuario y, por tanto, no fácilmente descifrable por terceros; disociar los datos incluidos dentro de un perfil de usuario para que, en el supuesto de acceso por personas no autorizadas, éstos no puedan acceder a los datos de los usuarios para emplearlos con fines malintencionados; idear diversas categorías de perfiles para controlar el volumen de datos personales que el usuario posibilita que sean visibles al resto de usuarios; y establecer diferentes categorías de autorizaciones fijadas por los propios usuarios para que puedan decidir quien puede visionar sus perfiles y, en su caso, a qué tipo de datos puede acceder.

Del mismo modo, deben ponerse a disposición de los usuarios medios a través de los cuales puedan denunciar situaciones que afecten a sus datos personales o de terceros o constituyan material inadecuado, ofensivo o ilícito. A tal efecto, en el seno de las redes sociales, podría crearse un sistema para que, de manera automática, se bloqueasen tales contenidos que, posteriormente, podrían ser objeto de examen por parte de personas físicas.

Resulta muy importante incidir en la idea de que el código de conducta que se apruebe debería limitar una práctica relativamente frecuente

por parte de las redes sociales cual es la reserva que éstas efectúan respecto a las políticas de privacidad en cuanto a que podrán modificarlas, de forma unilateral, sin necesidad de operar preaviso alguno a los usuarios ya registrados que inicialmente las hubieran aceptado. En el supuesto de que las modificaciones fueran necesarias deberían ser previamente comunicadas para que los usuarios puedan leerlas y, en su caso, aceptarlas, permitiéndoles, en todo caso, la posibilidad de darse de baja del servicio.

V. CONCLUSIONES

Internet es una red mundial y abierta que permite los intercambios de información. Actualmente, la *World Wide Web* se configura como un escenario de relaciones sociales fundamentado, en gran medida, en la participación creciente de los usuarios. Las redes sociales y, en general, los sitios *Web* colaborativos constituyen uno de los principales medios de contacto para, precisamente, fomentar la interacción con el resto de los usuarios de la red. Tales plataformas se basan en la creación de perfiles en los que los respectivos usuarios editan un importante número de datos personales. Sin embargo, es necesario lograr un equilibrio entre la naturaleza abierta de Internet y la protección de los datos personales de los usuarios de ésta.

Según los estudios empíricos más actuales, el número de usuarios de redes sociales crece de manera imparable a nivel mundial. En todo caso, debemos ser conscientes de que, a pesar del importante crecimiento y de la notoriedad de tales espacios sociales, los datos personales están sometidos a numerosos riesgos. Existen ciertas posibilidades a las que pueden recurrirse para eliminar y, en la medida de lo posible, mitigar estos últimos. Entre las mismas cabe destacar, por un lado, la regulación por parte de la normativa legal y, por otro, el fomento operado por esta última de la autodisciplina realizada por los agentes que en el sector que examinamos interactúan.

El valor de la autorregulación resulta especialmente relevante en un ámbito que, como el que analizamos, no parece conocer de fronteras territoriales. En efecto, las plataformas en las que las redes sociales se fundamentan, en no pocas ocasiones, se encuentran situadas fuera de la Unión Europea, principalmente en Estados Unidos, por lo que, en el momento del registro, los datos serán trasladados a los servidores y oficinas situados en ese país. Es, en consecuencia, necesario y plausible que las políticas de privacidad de las redes sociales que, en el espacio territorial mundial

existen, garanticen altos niveles de protección de la privacidad de los usuarios. Dado que, como ya hemos anticipado, Internet no conoce de fronteras de índole territorial, una vía en virtud de la cual puede alcanzarse, con elevados niveles de éxito, la finalidad mencionada es gracias a la autorregulación cuya manifestación más paradigmática son los códigos de conducta. Tales herramientas gozan de elevados niveles de eficacia en ámbitos parcialmente conexos al que hemos examinado –las redes sociales-, cual es el de la contratación electrónica y la publicidad interactiva.

En cuanto a los contenidos que los códigos de conducta reguladores de las redes sociales deberán abordar, desde el punto de vista de la protección de la privacidad de los usuarios, cabe decir que son extraordinariamente amplios. Una de las prerrogativas de tales documentos estriba en que mejorarán, de forma más o menos relevante, la normativa legal imperante respondiendo, asimismo, a cuestiones sobre las que no se ha pronunciado el legislador.

Es realmente loable, en este último sentido, que la Comisión Europea haya manifestado su intención de aprobar un código de conducta que reglamentará la privacidad en el ámbito de las redes sociales. No debemos perder de vista que uno de los caracteres de los códigos de conducta reside en su voluntariedad por lo que para que los usuarios puedan demandar el cumplimiento de su articulado habrá tenido que ser previamente asumido por la plataforma en cuestión. En todo caso, debe advertirse que su asunción comportará numerosas ventajas para la red social que se comprometa a su cumplimiento dado que, con tal actitud que será un elemento diferenciador respecto a sus competidores, podrá acreditar la observancia de las mejores prácticas en materia de protección de datos de sus usuarios.

BIBLIOGRAFÍA

ACEDO PENCO, Ángel (2006) "La responsabilidad civil extracontractual por atentados contra la dignidad divulgada mediante los servicios de la sociedad de la información en los ordenamientos comunitarios y español", *Anuario de la Facultad de Derecho*, núm. 24, pp. 97-117.

ALMUZARA ALMAIDA, Cristina COUDERT, Fanny MARZO PORTERA, Ana y NAVALPOTRO NAVALPOTRO, Yolanda (2008): *Estudio práctico sobre la protección de datos de carácter personal*, Valladolid, Lex Nova.

ÁLVAREZ-CIENFUEGOS SUÁREZ, José María (1999) *La defensa de la intimidad de los ciudadanos y la tecnología informática*, Aranzadi, Navarra.

ARENAS RAMIRO, Mónica (2003): "El derecho a la protección de datos personales: de la jurisprudencia del TEDH a la TJCE". En *25 Años de Constitución Democrática en España. Actas del Congreso celebrado en Bilbao los días 19 a 21 de noviembre de 2003*, Vol. 1, Bilbao, Servicio Editorial de la Universidad del País Vasco y GARCÍA HERRERA, Miguel A. (Ed.), pp. 575-588.

ARENAS RAMIRO, Mónica (2006) *El derecho fundamental a la protección de datos personales en Europa*, Tirant lo Blanch, Valencia.

ARRANZ ALONSO, Lucía (2003): "Los contratos del comercio electrónico". En MATEU DE ROS, Rafael y LÓPEZ-MONIS GALLEGO, Mónica (Coords.), *Derecho de Internet*, Navarra, Aranzadi, pp. 197-269.

BALLESTEROS MOFFA, Luis Ángel (2005) *La Privacidad Electrónica. Internet en el centro de protección*, Tirant lo Blanch, Valencia.

BENNET, Colin J. y RAAB, Charles D. (2006): *The Governance of Privacy: Policy Instruments in Global Perspective*, Cambridge (Londres), The MIT Press.

BENNET, Colin y RAAB, Charles (2006): *The governance of privacy. Policy instruments in global perspective*, Cambridge, The MIT Press.

BERGMAN, Eric (2000): *Information appliances and beyond: interaction design for consumer products*, Morgan Kaufmann.

BOCK, Andreas (2000): *Gütezeichen als Qualitätsaussage im digitalen Informationsmarkt*, Darmstadt, Toeche-Mittler.

CALVO ROJAS, Eduardo (2008): "Prólogo". En LESMES SERRANO, Carlos (Coord.), *La Ley de Protección de Datos. Análisis y comentario de su jurisprudencia*, Valladolid, Lex Nova, pp. 9-11.

CAMPUZANO TOMÉ, Herminia (2000): *Vida privada y datos personales*, Madrid, Tecnos.

CASTILLO JIMÉNEZ, Cinta (2002) "La sociedad de la información y los derechos fundamentales. Ley 34/2002 de servicios de la Sociedad de la Información y del comercio electrónico", *Derecho y Conocimiento: anuario jurídico sobre la sociedad de la información y del conocimiento*, núm. 2, pp. 21-37.

CHISSICK, Michael y KELMAN, Alistair (2002): *Electronic Commerce: Law and practice*, 3ª edición, Londres, Thomson.

COOLEY, Thomas (1888): *A Treatise on the Law of Torts or the Wrongs which arise independent of contract*, Chicago, Callaghan.

DEL PESO NAVARRO, Emilio RAMOS GONZÁLEZ, Miguel Ángel, DEL PESO RUIZ, Margarita y DEL PESO RUIZ, Mar (2008) *Nuevo Reglamento de Protección de Datos de Carácter Personal*, Madrid, Informáticos Europeos Expertos.

DÍAZ ARIAS, José Manuel (2008): *Guía práctica sobre normativa de protección de datos y publicidad comercial*, Barcelona, Ediciones Deusto.

EDELSTEIN, Judith Sharlin (2003): "Self-Regulation on Advertising: An Alternative to Litigation and Government Action", *IDEA: The Journal of Law and Technology*, Vol. 43, núm. 3, pp. 509-543.

ESPINOSA CALABUIG, Rosario (2001): *La publicidad transfronteriza*, Valencia, Tirant lo Blanch.

ETZIONI, Amitai (1999) *The limits of privacy*, New York, Basic Books.

FELIU ÁLVAREZ DE SOTOMAYOR, Silvia (2006): *La contratación internacional por vía electrónica con participación de consumidores. La elección entre la vía judicial y la vía extrajudicial para la resolución de conflictos*, Granada, Comares.

GELLMAN, Robert (1998): "Does privacy Law Work?". En AGREE Philip E. y ROTENBERG, M. (Eds.), *Technology and Privacy: The new Landscape*, Cambridge, The MIT Press.

GIERL, Heribert y WINKLER, Sabine (2000): Neue Gütezeichen als Qualitätssignale, *Marketing ZFP*, Vol. 1, núm. 3, pp. 197-207.

GÓMEZ CASTALLO, José Domingo (2001): "La asociación de autocontrol de la publicidad y la aplicación del principio de veracidad por su Jurado", *Estudios de Consumo*, núm. 57, pp. 133-146.

GONZÁLEZ DE LA GARZA, Luis M. (2008): *Sociedad de la Información en Europa*, Madrid, Reus.

GUERRERO PICÓ, María del Carmen (2006): *El impacto de Internet en el Derecho Fundamental a la Protección de Datos de Carácter Personal*, Madrid, Thomson Civitas.

HAROLD, Tipton y KRAUSE, Micki (2007): *Information Security Management Handbook*, CRC Press.

INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN (2008): *Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online*, Madrid, Publicaciones del Observatorio de la Seguridad de la Información.

JENSEN, Bil (2002): *Work 2.0: building the future, one employee at a time*, Perseus Publishing.

JULIÁ-BARCELÓ, Rosa, MARTÍNEZ MARTÍNEZ, Ricard y PANIZA FULLANA, Antonia (2008): *Protección de datos en Internet*, Barcelona, Publicaciones de la Universitat Oberta de Catalunya.

KROEBER-RIEL, Werner y WEINBERG, Peter (2003): *Konsumentenverhalten*, 8ª edición, Munich, Vahlen.

KUHLMANN, Eberhard (1990): *Verbraucherpolitik: Grundzüge ihrer Theorie und Praxis,* Munich, Vahlen.

LANGHEINRICH, Marc (2001) "Privacy by design Principles of Privacy Aware Ubiquitous Systems", http://www.vs.inf.ethz.ch/res/papers/privacy-principles.pdf.

LIN, Holin y SUN, Chuen-Tsai (2005) "The 'White-eyed' Player Culture: Grief Play and Construction of Deviance in MMORPGs", *Proceedings of DiGRA 2005 Conference*, Vancouver: DiGRA.

LÓPEZ JIMÉNEZ, David (2009a): "La autodisciplina del comercio electrónico: la Agencia de Calidad de Internet como paradigma de referencia" (Parte I), *Revista de Autocontrol de la Publicidad*, núm. 141, pp. 10-14.

LÓPEZ JIMÉNEZ, David (2009b): "La autodisciplina del comercio electrónico: la Agencia de Calidad de Internet como paradigma de referencia" (Parte II), *Revista de Autocontrol de la Publicidad*, núm. 142, pp. 9-14.

LUCAS MURILLO DE LA CUEVA, Pablo (1999): "La construcción del derecho a la autodeterminación informativa", *Revista de Estudios Políticos*, 104, pp. 35-60.

MARTOS, Juan Jesús (2005) "DNI electrónico: obligaciones jurídicas para el titular y límites constitucionales en el derecho fundamental a la intimidad y a la protección de datos", *Revista Aranzadi de Derecho y Nuevas Tecnologías*, núm. 9, pp. 79-91.

Multi-State Working Group on Social Networking of State Attorneys General of the United States (2008) *Enhancing Child Safety & Online Technologies*, Harvard Law School.

MUÑIZ CASANOVA, Natalia y ARIZ LÓPEZ DE CASTRO, Eneko (2004) "Los datos personales en el desarrollo de la actividad". En MARZO PORTERA, Ana y RAMOS SUÁREZ, Fernando María (Dirs.), La *Protección de Datos en la Gestión de Empresas*, Thomson Aranzadi, Navarra, pp. 85-118.

OLIVIER LALANA, Ángel Daniel (2002) "El derecho fundamental "virtual" a la protección de datos. Tecnología transparente y normas privadas", *La Ley*, núm. 5, Julio, pp. 1539-1546.

PATIÑO ALVES, Beatriz (2007): *La autorregulación publicitaria. Especial referencia al sistema español*, Barcelona, Bosch.

PAZ-ARES RODRÍGUEZ, Cándido (2000): "El comercio electrónico. (Una breve reflexión de política legislativa)". En MATEU DE ROS CEREZO, Rafael y CENDOYA MÉNDEZ DE VIGO, Juan Manuel (Coords.), *Derecho de Internet, Contratación electrónica y firma digital*, Navarra, Aranzadi, pp. 85-98.

PIÑAR MAÑAS, José Luis (2008a): *¿Existe la privacidad? Inauguración del curso académico 2008/2009*, Madrid, Publicaciones de la Fundación Universitaria San Pablo CEU.

PIÑAR MAÑAS, José Luis (2008b): "El derecho fundamental a la protección de datos. Contenido esencial y retos actuales. En torno al nuevo Reglamento de Protección de Datos". En PIÑAR MAÑAS, José Luis y CANALES GIL, Álvaro, *Legislación de Protección de Datos*, Madrid, Iustel.

PRIETO ANDRÉS, Antonio (2002) "La nueva Directiva europea sobre el tratamiento de datos personales y la protección de la intimidad en el sector de las telecomunicaciones", *La Ley*, núm. 5, Septiembre, pp. 1710-1713.

PUNZÓN MORALEDA, Jesús y SÁNCHEZ RODRÍGUEZ, Francisco (2004): "El nuevo papel del Estado ante la regulación en Internet", *Revista de la Contratación Electrónica*, núm. 55, pp. 63-78.

REBOLLO DELGADO, Lucrecio (2008): *Vida privada y protección de datos en la Unión Europea*, Madrid, Dykinson.

RODRÍGUEZ CÁRCAMO, Juan Manuel (2005) "Protección de datos de carácter personal". En DE FUENTES BARDAJÍ, Joaquín (Dir.) y PEREÑA PINEDO, Ignacio (Coord.), *Manual de Derecho Administrativo Sancionador*, Thomson Aranzadi y Ministerio de Justicia, Navarra, pp. 1725-1751.

RODRÍGUEZ LÓPEZ DE LEMUS, Pedro y BORREGO ZABALA, Bartolomé (2008): *Las empresas ante la normativa sobre protección de datos. Exigencias del nuevo Reglamento de desarrollo de la Ley Orgánica de Protección de Datos (RD 1720/2007)*, Sevilla, Cámara de Industria, Comercio y Navegación de Sevilla.

ROSEN, Larry (2006) "Adolescents in MySpace: Identity Formation, friendship and sexual predators", http://www.csudh.edu/psych/Adolescents%20in%20MySpace%20%20Executive%20Summary.pdf.

ROSSNAGEL, Alexander (2003): *Handbuch Datenschutrecht,* München, Verlag C.H. Beck.

RUIZ NÚÑEZ, Mariola (2003): "Códigos de Conducta". En CREMADES GARCÍA, Javier y GONZÁLEZ MONTES, José Luis (Coords.), *La Nueva Ley de Internet (Comentarios a la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico)*, Madrid, La Ley, pp. 295-307.

RUSSELL, Thomas y LANE, Ronald W. (2002): *Kleppner´s Advertising Procedure*, Upper Saddle River, Prentice Hall.

SAMPOL PUCURRULL, M. (2005): "Administración Electrónica". En DE FUENTES BARDAJÍ, Joaquín (Dir.) y PEREÑA PINEDO, Ignacio (Coord.), *Manual de Derecho Administrativo Sancionador*, Navarra, Thomson Aranzadi y Ministerio de Justicia, pp. 1753-1776.

SERRA RODRÍGUEZ, Adela (2000) "Los derechos de los particulares en la nueva Ley de protección de datos de carácter personal", *La Ley*, Vol. 6, http://www.laley.net.

SHAPIRO, Andrew (2002): "Herramientas para la democracia". En MAYOR MENÉNDEZ, Pablo y AREILZA CARVAJAL, José (Coords.), *Internet, una profecía*, Barcelona, Ariel, pp. 15-32.

SIRINELLI, Pierre (1998) : "L´adequation entre le village virtual et la creation remise en cause du role de l'Etat?". En BOELE-WOELKI, Katharina y KESEDJIAN, Catherine (Eds.), *Internet, Which Court Decides? Which Law Applies? Quel Tribunal Decide? Quel Droit S'applique?*, La Haya, Kluwer Law Internacional, pp. 1-22.

SMITH, Robert Ellis (1993): *War stories: accounts of persons victimized by invasions of privacy*, Privacy Journal.

SOLOMON, Michael R. (2003): *Conquering consumerspace: marketing strategies for a branded world*, AMACOM Div American Mgmt Assn.

SOLOVE, Daniel (2004): *The Digital Person. Technology and Privacy in the Information Age*, New York, New York University Press.

TOLCHINSKY, Paul D. MCCUDDY, Michael K. ADAMS, Jerome, GANSTER, Daniel C. y FROMKIN, Howard L. (1981): "Employee perception of invasion of privacy: A Field Simulation Experiment", *Journal of Applied Psychology*, núm. 66, pp. 308-313.

VÁZQUEZ IRUZUBIETA, Carlos (2002): *Comercio Electrónico, Firma electrónica y servidores*, Madrid, Dijusa.

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