El recurso a las redes sociales por parte de la Administración Pública: incidencia de la autorregulación en beneficio de la privacidad del destinatario[1]

Dr. David López Jiménez
Universidad Autónoma de Chile

Dra. Patricia Vargas Portillo
Universidad Autónoma de Chile

Congreso Derecho TICs-SICARM 2014
Innovación, tecnología y gestión avanzada de la información administrativa
Implicaciones jurídicas del cambio de paradigma
Facultad de Derecho. Universidad de Murcia
23 y 24 de octubre de 2014

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, las redes sociales electrónicas suponen un destacable avance con sugerentes proyecciones en diferentes planos. Recurren a dichas plataformas no solo los particulares, sino, también, las empresas y las Administraciones Públicas. 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 satisfactoria, es mediante la autorregulación. En virtud de este último fenómeno, se han elaborado, por parte de diversas Administraciones Públicas, documentos de buenas prácticas sobre la materia. Estos últimos se erigen en un sugerente complemento de la normativa legal.

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. Nowadays, social networking sites suppose a major breakthrough with suggestive projections in different fields. These platforms are used not only by individuals, but also by companies and public administrations. In any case, significant problems for the protection of personal data arise. A tool that can be used to solve this issue satisfactorily is the self-regulation. Because of this phenomenon, different public administrations have prepared best practice documents on the subject. In this sense, this type of information establishes an attractive complement to legal regulations.

Palabras clave: "Administración Pública";"autorregulación"; Internet"; "privacidad"; "redes sociales".

Keywords: "Public Administration"; "self-regulation"; "Internet"; "privacy"; "social networks".

[1] Esta comunicación ha sido elaborada en el marco del Proyecto de investigación FONDECYT N° 11130188, del que el Dr. David López Jiménez es Investigador Principal.

1. 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, en ocasiones, 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[2]. Sin perjuicio de que en la presente comunicación nos referiremos, con carácter general, a esta materia, también tomaremos conciencia del uso que de estas plataformas están operando las Administraciones Públicas. Estas últimas, con carácter general, y en particular los Ayuntamientos, como Administración más cercana al ciudadano, como venimos comentando, están comenzando a recurrir, cada vez en mayor medida, a estas plataformas para comunicarse mejor, pero también para mejorar la relación con el ciudadano eincrementar la calidad de los servicios públicos que se ofrecen.

Hace ya una década, determinó el presidente y cofundador de *Sun Microsystems*, Scott MCNEALY, que debemos ser conscientes de que no tenemos privacidad[3]. Matizando tal afirmación, posteriormente, ha llegado a afirmar, a juicio de cierto sector de la doctrina[4], de manera igual de descorazonadora, que si gozamos de privacidad es porque alguien tolera que la tengamos. Hay quien[5], incluso, ha llegado a manifestar que un exceso de privacidad podría ser contraproducente para la sociedad, proponiendo un concepto comunitario de privacidad que 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[6] como la propia jurisprudencia[7]. Una definición muy

---

[2] SMITH (1993): 7.

[3] 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; SOLOVE (2004): 224; BENNET y RAAB (2006): 298; HAROLD y KRAUSE (2007): 2764.

[4] PIÑAR MAÑAS (2008a): 5.

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

[6] GELLMAN (1998): 193.

extendida, aunque ya superada, es la que a finales del siglo XIX pronunció el juez americano Cooley[8] que manifestó que privacidad es el derecho a estar solo, a estar en paz ("*therightto 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*[9], 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[10].

La irrupción de las nuevas tecnologías de marcado carácter social 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[11] que permite a sus usuarios acceder y participar en la creación de un conocimiento ilimitado. Nos encontramos ante un escenario sometido a frecuentes violaciones de la privacidad. En el presente estudio nos limitaremos al análisis de la privacidad en el ámbito de las redes sociales.Sin perjuicio de que abordaremos esta cuestión, con carácter general, posteriormente, nos centraremos en el recurso de estas plataformas por parte de las Administraciones Públicas y los eventuales problemas que, en este concreto aspecto, pueden suscitarse. Finalmente, veremos la incidencia que, a este respecto, suscita el fenómeno de la autorregulación.

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

---

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

[8] COOLEY (1888): 29.

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

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

[11] 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.

[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).

[13] LANGHEINRICH (2001); BALLESTEROS MOFFA (2005).

[14] ÁLVAREZ-CIENFUEGOS SUÁREZ (1999).

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.

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-, sino a que las propias empresas valoran, de manera importante, la preocupación que los ciudadanos, en general, manifiestan respecto a su privacidad[18].

El Consejo de Europa[19] primero y el ordenamiento jurídico comunitario[20] 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

[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]JULIÁ-BARCELÓ, MARTÍNEZ MARTÍNEZy PANIZA SULLANA (2008): 5.
[19] 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. En cuanto a esta última cuestión, nos remitimos a las consideraciones de ARENAS RAMIRO (2003): 576-580.
[20] 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 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.

mercado europeo que facilite el libre intercambio de personas, mercancías, servicios y capitales, no sólo se encuentran en Directivas comunitarias[21] de notable relevancia, ya que fueron incluidas en el artículo II-68[22] del Tratado por el que se establecía una Constitución para Europa que, como es sabido, fue sustituido por el Tratado de Lisboa de 13 de diciembre de 2007[23].

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[24]- fundamentándolo en el art. 18.4 de la Constitución Española.

3.LA PRIVACIDAD Y LAS REDES SOCIALES: CONCEPTO, MODALIDADES, AMENAZAS Y RECURSO POR PARTE DE LA ADMINISTRACIÓN PÚBLICA

El derecho fundamental a la protección de datos, regulado específicamente en el art. 18.4 de la Constitución Española, que ha de diferenciarse[25] 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, se ha constatado que quienes tienen la sensación 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

[21] 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-.

[22] 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 concretos 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".

[23] 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.

[24] 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.

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

quienes pueden tener la sospecha de que han perdido el control sobre los mismos[26]. 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[27].

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[28].

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.

La necesidad de regular, tanto en virtud de normas legales como, por efecto de estas últimas, por medio de acuerdos privados, la protección de datos de carácter personal 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[29]) 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.

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.

3.1. Concepto de red social

[26] 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.

[27] PIÑAR (2008a): 11.

[28] Nos encontramos ante un aspecto destacado por el *Multi-StateWorkingGroupon Social Networking of StateAttorneys General of theUnitedStates* que, el 31 de diciembre de 2008, ha hecho público el estudio cuyo título es *EnhancingChild Safety & Online Technologies*.

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

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 *WebClassmates* 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). El número de usuarios de tales plataformas de comunicación crece a un ritmo, sencillamente, de vértigo. 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[30] en el que un número inicial de participantes, a través del envío de invitaciones por medio de correos electrónicos[31], 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 definiciones 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[32] 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[33], PDA, etc.- que posibilitan que los usuarios puedan diseñar

[30] 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 LIN y SUN (2005).

[31] 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*-.

[32] 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.

[33] 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

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.

3.2. 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 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.

3.2.1. 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.

1. 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

---

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*).

los mencionados contenidos, y, en ciertos casos, otorgar puntuaciones. Cabe citar, a título de ejemplo, *Youtube*, *Dalealplay.com* y *Google Vídeo*.

2. 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.

3. 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*.

3.2.2. 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*.

3.3. 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:

1. 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 configure correctamente, por

lo que determinados datos[34] 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[35]. 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.

2. 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[36], 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 retirada inmediata[37]. 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 instrumentos derivados de la autorregulación.

---

[34] 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 relativos a la ideología, religión y vida sexual. Sobre esta cuestión, incideel documento de opinión 5/2009, de 12 de junio, emitido por el grupo de trabajo del Artículo 29, respecto a las redes sociales.

[35] 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.

[36] 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.

[37] 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.

3. 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[38], 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[39] generados por los propios usuarios en el sistema para, posteriormente, emplearlos como 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:

1. La recepción de correos electrónicos no solicitados o, en terminología anglosajona, *spam*[40]. 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[41], 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 remitan*spam*, parezca que se envía desde los contactos directos[42]. 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

[38] 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.

[39] 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.

[40] 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 –*spicedham*- junto con las compras que se efectuaban en las carnicerías haciéndose, de esta forma, mención de un producto recibido sin ser, en principio, deseado.

[41] 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 -*ControllingtheAssault of Non-SolicitedPornography and Marketing Act*-. La sanción no cabe duda que tendrá un importante efecto disuasorio de cara a posibles infractores futuros de la norma mencionada.

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

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 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.

2. 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 o 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.

3. Ser víctima de prácticas manifiestamente delictivas como el *phishing*[43] y *pharming*[44]. Por paradójico que pueda resultar, es frecuente que los usuarios

[43] 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*.

[44] 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.

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, aún más si cabe, cuando los usuarios tienen la misma contraseña para efectuar operaciones financieras[45].

4. La indexación de perfiles, en todo caso, no permitida, por parte de buscadores electrónicos[46]. En numerosas ocasiones, las redes sociales posibilitan que los motores de búsqueda indexen en sus exploraciones los perfiles de los usuarios[47], junto con información personal y otros contactos vinculados, lo que supone un importante riesgo para la privacidad[48] además de, naturalmente, dificultar el proceso de eliminación de su información en Internet.

5. Violaciones de identidad. Un fenómeno relativamente reciente 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.

3.4. Uso por parte de las Administraciones públicas

Resulta incuestionable, a nivel global, las bondades del uso de Internet. En este sentido, como hemos puesto de manifiesto,es patente que el recurso de la denominada Web 2.0, dentro de la que se incluyen las redes sociales,tiene cada vez más prerrogativas. Así, su empleo, por parte de la Administración[49], representa una nueva vía de comunicación (fácil, rápida y económica) e intercambio de múltiples experiencias con los ciudadanos, que permite diversos objetivos. Entre los mismos, podemos enunciar, sin ánimo agotador, los tres siguientes: generar áreas de discusión y concienciación ciudadana; coadyuvar a la prestación de servicios públicos con un mayor grado de eficiencia, eficacia y transparencia; y, finalmente, es un nuevo medio accesible, de uso sencillo y alta implementación, en el plano social, que, entre otros factores, permite que el gobierno puedadifundir diversa información relativa a su gestión, políticas públicas y las actividades desarrolladas, lo que, qué duda cabe, contribuye a la transparencia. Uno de los mayores desafíosde la Administración Pública,

[45] 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.

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

[47] Consciente de los problemas que venimos comentando, el Grupo internacional sobre protección de datos en las telecomunicacionesadoptó 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.

[48] 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.

[49] Numerosos organismos de la Administración Pública española cuentan con perfiles en múltiples canales susceptibles de integrarse en la denominada Web 2.0. Así, podemos referirnos a su presencia en YouTube, Twitter, Facebook y la creación de diversos blogs.

estriba, en cualquier caso, en asegurar diferentes aspectos cual es la privacidad, la seguridad y la protección de los datos personales de los usuarios con los que la misma se interrelaciona a través de los perfiles creados en las redes sociales (nos referimos a los ciudadanos).

Además de permitir la participación del ciudadano, las redes sociales mejoran las vías de comunicación de la Administración[50]. Si bien es cierto que los sitios Web de las Administraciones públicas incluyen información actualizada, las redes sociales también contribuyen a otros extremos. En este sentido, entre otros aspectos, dichas plataformas sirven paradar respuestas a los usuarios, que gozarán de cierta celeridad –a diferencia de otros mecanismos de contacto con la Administración-. Igualmente, debe considerarse que la información que se incluye puede ser de utilidadpara otros individuos que estén en la misma situación. Todo cuanto señalamos tiene lugar de una forma que goza de una mayor cercanía para el destinatario. Las plataformas digitales de las que nos ocupamos tienen la bondad de redireccionar a los ciudadanos hacia el sitio Web corporativo[51]con la finalidad de ampliar la información oficial.Finalmente, debe reseñarse que las redes sociales posibilitan la creación de redes temáticas de usuarios que, a su vez, dan lugar a conocimientos complementarios que hace posible que la organización tome conciencia de sus intereses y la información presente en estas redes para, de este modo, poder tenerlos en consideración.

Cuando la Administración Pública recurre a las redes sociales se espera un comportamiento ético de la misma, pero también que cumpla las disposiciones legales. Igualmente, es preceptivo que respete las normas y políticas de uso de la de la red social de que se trate[52]. En el caso de que existan instrumentos de autorregulación, los mismos deberán observarse –con carácter complementario-.

En todo este ámbito de cuestiones que venimos comentando, debemos considerar que la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, -LAECSP-, ha establecido el derecho de éstos a comunicarse con las Administraciones públicas a través de medios electrónicos[53], pero, simultáneamente, determina que la Administración ostenta la obligación de poner los medios adecuados para garantizar la protección de datos[54].Desde los principios generales esta Ley, pone de relieve que debe procurarse en la implementación de las relaciones electrónicas con el ciudadano, el derecho a la protección de datos de carácter personal en los términos establecido en la LOPD.

---

[50] A este respecto, podemos referirnos a la atención telefónica y presencial.

[51] Ahora bien, además de al sitio Web corporativo de la Administración, cabe la posibilidad de que se dirija al usuario hacia otro link que proporcione información tan fiable como la generada por las vías oficiales.

[52] Se trata, entre otras, de las políticas de privacidad, las normas de publicidad y condiciones de uso.

[53] Resulta propio a la Administración electrónica el empleo de la informática y las redes de telecomunicaciones para que el ciudadano tenga la posibilidad de acceder, de forma digital, a la información, a los servicios públicos pero, también, para que el mismo pueda presentar su solicitud, desde cualquier lugar, de manera virtual.

[54] Debe repararse que la puerta a esta modalidad de Administración puede estimarse abierta con carácter previo a la entrada en vigor de esta Ley que, dicho sea de paso, podemos ejemplificar en dos normas. En primer lugar, la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común ya introducía, en el art. 45, el primer impulso a la utilización de medios electrónicos, ofreciendo, de esta manera, la posibilidad a las Administraciones de utilizarlos en el ejercicio de sus funciones, siempre que dispusieran de los medios técnicos necesarios. En cualquier caso, en esa etapa, la Administración pública española estaba muy alejada, al igual que el ciudadano de ese periodo temporal, del uso de las nuevas tecnologías. En segundo lugar, la Ley 24/2001, de 27 de diciembre, de Medidas Fiscales, Administrativas y del Orden Social que efectúa varias reformas sobre el articulado de la ley antes enunciada que convierte a la Administración física en una que, además de ser tradicional, también es electrónica.

La inobservancia de la normativa legal que impera en toda esta materia –relativo a la privacidad, comunicaciones comerciales, competencia desleal y propiedad intelectual- puede llegar a determinar responsabilidad patrimonial por parte de la Administración Pública[55].

Asimismo, debe ponerse de manifiesto que la Administración Pública –sobre todo aquella que tiene carácter local-, en el uso de las redes sociales digitales,gestiona un importante volumen de datos personales de los ciudadanos. Dicha información es solicitada esencialmente en virtud de diversos cuestionarios y formularios realizados de manera virtual. Sin embargo, no tutelan, de manera efectiva, el control relativo al uso y destino de tales datos personales. De hecho, existe la posibilidad de que tales datos sean objeto de cesión a terceros e incluso, en algunos casos, obtenidos por fallos de seguridad.

En materia de protección de datos de carácter personal, la Administración ha de informar a los usuarios de las redes sociales de una serie de cuestiones. A este respecto, necesariamente debe poner de relieve: los fines de la recogida de los datos; si los datos personales serán objeto de cesión a otras entidades; garantía preceptiva del deber de confidencialidad; observancia de las medidas de seguridad necesarias para impedir el acceso no permitido de terceros; existencia de una política de privacidad que tenga en consideración los principios del derecho de protección de datos de carácter personal[56].

En suma, la penetración del derecho a la protección de datos de carácter personal en el espacio de la Administración pública determina que las mismas deban efectuar una modificación tanto de sus procedimientos como de su actuación[57].

4. LA AUTORREGULACIÓN COMO ESTRATEGIA ORDENADORA COMPLEMENTARIA: INSTRUMENTOS DE BUENAS PRÁCTICAS EN LA ADMINISTRACIÓN PÚBLICA

4.1. Consideraciones previas

La autorregulación constituye 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 con carácter general, el comercio electrónico, dentro del que pueden considerarse incluidas las redes sociales.

Debe ponerse de manifiesto que la autorregulación es una figura encarecidamente sugerida por el legislador, comunitario[58], estatal[59] y autonómico[60], en

[55] De hecho, cuando el incumplimiento tuviera lugar por parte bien de personal como de empresas externas cuyos servicios hubieran sido contratados por la Administración, las mismas podrán tener que responder a efectos administrativos, civiles o penales. En relación a esta sugerente materia, nos remitimos a lo previsto por el art. 31 bis del Código Penal español.

[56] Nos referimos esencialmente a los siguientes principios: consentimiento, información, calidad de los datos personales, finalidad, observancia de los niveles o grado de seguridad, y, finalmente, posibilidad del ejercicio de los derechos de acceso, rectificación, cancelación y oposición (derechos ARCO).

[57] Todo ello con el objetivo, entre otros aspectos, de observar la normativa actualmente imperante y mejorar la imagen que los ciudadanos tienen respecto a la Administración.

diferentes textos normativos. Uno de los ámbitos en los que puede alcanzarse la vigencia de la fórmula reguladora que analizamos, es, como seguidamente veremos, 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 determinada 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. En definitiva, la presencia de tales prerrogativas hace del mismo un sistema verdaderamente eficaz y aconsejable en el ámbito de las redes sociales[61].

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.

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 poder legislativo de sus obligaciones, sino como complemento[62] a una legislación que, inevitablemente, no puede dejar de tener un carácter ciertamente general y ambiguo.

---

[58] 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.

[59]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.

[60]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.

[61]EDELSTEIN (2003): 509-543; FELIU ÁLVAREZ DE SOTOMAYOR (2006).

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

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 las redes sociales.

En los últimos años, somos testigos y, en ciertos casos, protagonistas de un vigoroso impulso, fomentado desde diversas instancias, del *softlaw*[63] –en terminología anglosajona- o derecho no vinculante especialmente por lo que respecta a la protección de los consumidores y/o usuarios en Internet. 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 determinadas prácticas[64]. 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 sugeridopor parte de instancias públicas.

Es conveniente, en este sentido, poner de manifiesto que los instrumentos de autodisciplina (como, entre otros, es el caso de 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.

4.2. Instrumentos de buenas prácticas: los códigos tipo

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[65]. 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 fomentar, en primer término, la creación de instrumentos derivados de la autodisciplina. Las herramientas instauradas en este último sentido, deben ser parte de una adecuada estrategia de actuación en la Web 2.0 por parte de la Administración pública. En virtud de esta última, podrán alcanzarse, de forma satisfactoria, diversos objetivos. Entre los mismos, podemos mencionar, sin ánimo agotador, los siguientes: observancia de la normativa legal imperante y prevención de eventuales sanciones que puedan repercutir, de manera negativa, en su imagen y/o reputación de carácter digital; disciplinar, de la manera más precisa posible, las normas o reglas relativas al comportamiento tanto del personal, con carácter general, comodel responsable de

[63] Sobre las diferencias que existen entre las normas jurídicas o *hardlaw* y las normas de carácter deontológico o *softlaw*, nos remitimos a las consideraciones de, entre otros autores, PAZ-ARES RODRÍGUEZ (2000): 85-98; SHAPIRO (2002): 15-32.
[64]ESPINOSA CALABUIG (2001); ARRANZ ALONSO (2003): 197-269; PATIÑO ALVES (2007).
[65] PIÑAR MAÑAS (2008b): 91.

atención al cliente –popularmente conocido como *comunity manager*- en cuanto a la forma de actuar en las redes sociales[66]; vinculado con el objetivo previo, cabe referirse al hecho de ostentar una política que revele la forma de comportarse ante las situaciones que puedan llegar a plantearse. En virtud de la misma, el personal de la Administración pública podrá tomar una conciencia clara de la manera de actuar, lo que, a su vez, mejorará, de manera notable, la coordinación y la gestión de las actuaciones que se acometan. La concurrencia de una estrategia de actuación uniforme transmitirá valores tan significativos como la confianza y la seguridad, dando lugar, asimismo, a una imagen de coherencia en el plano virtual[67].

Existen diversos ejemplos que ponen de relieve la presencia de instrumentos de autodisciplina, relativos a las redes sociales, en el ámbito de la Administración Pública española. En este sentido, podemos referirnos, sin ánimo exhaustivo, a los siguientes supuestos: la guía que disciplina el comportamiento de la Administración pública británica en *Twitter*;la guía relativa a los usos y estilo en las redes sociales por parte del Gobierno Vasco; la guía relativa a los usos y estilo en las redes sociales por parte de la Generalitat de Cataluña; guía relativa a los usos y estilo en las redes sociales por parte del Gobierno de Canarias; guía relativa a los usos y estilo en las redes sociales por parte de la Junta de Castilla y León; y la política de uso de redes sociales electrónicas en el Ayuntamiento de Madrid[68].

En un contexto territorial diverso –en concreto el de América Latina-, interesa reseñar que, hace relativamente poco tiempo, se publicó la denominada Declaración de Santiago rubricada "Hacia la unificación de criterios sobre seguridad y protección de datos en Internet". Estamos frente a una iniciativa procedente del Observatorio Iberoamericano de Protección de Datos presentada en Santiago de Chile el pasado 12 de septiembre de 2013. Dicho documento, entre otros extremos, busca fijar las bases de lineamientos comunes en el ámbito de la seguridad y la salvaguarda de los datos de carácter personal. Todo ello por parte de empresas como de las Administraciones públicas de América Latina.

Si bien en sede de instrumentos de autorregulación en el ámbito de la salvaguardia de los datos de carácter personal, en el uso de las redes sociales, por parte de la Administración Pública, cabría aludir a diversos supuestos, seguidamente, únicamente nos referiremos a algunos de ellos como paradigma sobre el particular.

---

[66] Todo cuanto se comenta resulta especialmente importante en cuanto a la gestión de una eventual crisis de comunicación.

[67] Es de notable relevancia la concienciación y capacitación de los trabajadores públicos en la tutela de los datos de carácter personal. Estamos frente a un tema que se incluye en la Disposición Adicional 2º de la LAECSP, al referirse a la necesidad de formación de los trabajadores públicos tanto en la protección de datos como en el uso correcto de los medios electrónicos en la actividad administrativa. Considerando la definición que de medio electrónico opera la citada norma, a saber: "mecanismo, instalación, equipo o sistema que permite producir, almacenar o transmitir documentos, datos e informaciones; incluyendo cualesquiera redes de comunicación abiertas o restringidas como Internet, telefonía fija y móvil u otras" cabe considerar que dicha norma legalserá de aplicación a la red social digital.

[68] En materia de protección de datos, el citado documento se remite a la aplicación de la instrucción 2/2010 de adopción de medidas de adaptación a la Recomendación 2/2008, de 25 de abril de la Agencia de Protección de Datos de la Comunidad de Madrid, sobre publicación de datos personales en boletines y diarios oficiales en internet, en sitios web institucionales y en otros medios electrónicos y telemáticos, aprobada por Resolución de 27 de diciembre de 2010 del Director General de Calidad y Atención al Ciudadano y publicada en el Boletín Oficial del Ayuntamiento de Madrid de 3 de enero de 2011.

Antes de entrar en materia, debemos precisar que, como seguidamente veremos, existe un común denominador en cuanto a que se recurre a la figura de códigos tipo[69]. Estos últimos tienen un papel fundamental para encontrar el equilibrio entre la aplicación de las nuevas tecnologías y el control de la privacidad, instrumentando la autorregulación a través de acuerdos incluidos en los mismos. La adhesión a un determinado código tipo pone de manifiesto el compromiso, por parte de la entidad –que podrá ser la Administración Pública- que asume su respeto[70], del cumplimiento del articulado contenido en el mismo. Este último incluirá la propia normativa legal –que ajustará a ciertos escenarios- más, en numerosas ocasiones, determinadas previsiones más garantistas que las reconocidas, con carácter mínimo, por el legislador.

Los códigos tipo, en el caso de España, son objeto de atención por parte del art. 32 de la LOPD[71], por el Título VII –arts. 71 a 78-, así como por el capítulo VI del Título IX del Reglamento de desarrollo de la LOPD –arts. 146 a 152- donde se determinan los requisitos, formales y de fondo, que los mismos han de reunir. Cabe advertir que el título regulador de los códigos tipo, comprendido en el nuevo Reglamento de desarrollo de la LOPD, constituye una de las materias en las que se han introducido más novedades, con respecto al régimen jurídico anterior, y más mecanismos dirigidos a facilitar y simplificar el cumplimiento de la legislación sobre protección de datos a través de la autorregulación.

A este último respecto, debe precisarse que el articulado del código tipo debe, a nuestro entender, incluir compromisos firmes susceptibles de verificación[72] que, además, deberán ser analizados en cada supuesto concreto. *A sensu contrario*, las normas contenidas en el mismo no han de ser simples declaraciones programáticas que no vinculen a sus firmantes ni sean susceptibles de revisión por el organismo de control instaurado para garantizar la observancia del código tipo por parte de las entidades que deseen adherirse al mismo[73]. En otros términos, el compromiso firme se contrapone a la simple aspiración. Debemos también insistir en que podríamos plantearnos el supuesto de qué acontecería si las normas de los códigos tipo estuvieran redactadas de forma que se aproximen más a esta última acepción. Pues bien, tales supuestos no reunirán los caracteres necesarios para, precisamente, generar un compromiso firme. No olvidemos que los códigos tipo tienen como finalidad elevar el nivel de protección, en materia de privacidad, más allá de lo dispuesto por el legislador[74]. Naturalmente, los códigos tipo que reproducen, sin más, la norma no incurren en mejora de ningún tipo. Respecto de

[69] Deben diferenciarse, y no confundirse, código de conducta y código tipo. Se trata de conceptos, aunque relacionados, diversos, pues para que un código de conducta sea considerado código tipo deberá acreditar el cumplimiento de diversos extremos. Así, podemos adelantar que todo código tipo será código de conducta, pero no todo código de conducta será código tipo. En otros términos, los códigos de conducta podrían ser considerados el género, mientras que los códigos tipo serían la especie.

[70] En el ámbito laboral no falta quien ha querido ver una remisión equívoca, pero necesaria, a la negociación colectiva laboral -cada vez más preocupada por todo lo relativo a las nuevas tecnologías- como instrumento para precisar una materia todavía de escasa consideración en el mundo de la empresa, así como para asignar un papel activo a los representantes de los trabajadores, los cuales quedan prácticamente olvidados en el texto de la LOPD. En este sentido, CARDONA RUBERT (2004), p. 2.

[71] Tal precepto se refiere a los códigos tipo, estableciendo que podrán incluir "las condicionesde organización, régimen de funcionamiento, procedimientos aplicables, normas deseguridad del entorno, programas o equipos, obligaciones de los implicados en el tratamientoy uso de la información personal, así como las garantías en su ámbito, para el ejercicio de losderechos de las personas con pleno respeto de los principios y disposiciones de la presenta Leyy sus normas de desarrollo".

[72] Un enunciado resulta verificable si es posible una comprobación, positiva o negativa, de su contenido en condiciones adecuadas, prescindiendo de las dificultades meramente técnicas.

[73] Es más, la verificabilidad del compromiso significa que pueda ser controlado.

[74] Ahora bien, la mejora sobre la propia normativa puede derivarse bien del propio contenido sustantivo del código tipo bien de la existencia de un sistema de control de esa reglas y resolución de conflictos, por considerarse más ágil que los propios sistemas públicos (judiciales o administrativos).

esas reglas, no hay compromiso voluntariamente asumido, sino simple cumplimiento de una norma legal, en nuestro caso en el ámbito de la protección de datos de carácter personal.

En primer término, cabe referirse al Manual de buenas prácticas para entidades locales de la Comunidad Autónoma del País Vasco[75] en el ámbito de la tutela de los datos de carácter personal. Su objetivo fue, precisamente, el de adecuar lo contemplado en la legislación relativa a la protección de datos de carácter personal a las particularidades de los tratamientos efectuados por parte de las entidades locales del País Vasco. Mediante este tipo de instrumentos, se alcanza, entre otros aspectos, un mayor grado de concienciación en materia de protección de datos de carácter personal por parte de las entidades locales y, por ende, de los sujetos que trabajan en la misma. Resulta significativo poner de manifiesto que se trata de un código tipo al que pueden adherirse las entidades locales del País Vasco que así lo decidan. Se trata de un código tipo en un Registro Autonómico de Protección de Datos e incluido, asimismo, en el Registro General de Protección de Datos.

En segundo lugar, cabe destacar el código tipo de la Universidad de Castilla La Mancha. Como la Exposición de Motivos del citado documento pone de relieve, el mismo persigue un triple objetivo, a saber: cumplir de la forma más sencilla y segura con la legislación correspondiente a través de un documento único que reúna todos los elementos esenciales; aumentar la protección de los datos personales almacenados en ficheros automatizados incrementando las medidas de seguridad legalmente exigidas, y servir como material educativo para la comunidad universitaria, con especial interés en los alumnos.

En tercer y último lugar, podemos referirnos al código tipo de Confianza Online, que es una asociación sin ánimo de lucro de carácter privado. Si bien el mismo se refiere, de manera específica, al ámbito digital, son muy reducidas las Administraciones públicas que se han adherido al mismo[76].

En definitiva, consideramos que los códigos tipo se erigen en sugerentes instrumentos de autorregulación, puestos en práctica por la Administración pública, susceptibles de garantizar la protección de los datos de carácter personal de los ciudadanos en el ámbito de las redes sociales.

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.

---

[75] Dicho documento es fruto de una actividad conjunta y coordinada por parte de las siguientes instituciones: la Agencia Vasca de Protección de Datos; la Asociación de Municipios Vascos; y los siguientes Ayuntamientos: Vitoria, Gasteiz, Basauri, Getxo, Ermua, Eibar y Beasain.

[76] En este sentido, podemos, entre otras, referirnos a la Caixa Andorrana de Seguretat Socia y la Cámara de Comercio e Industria de Zaragoza.

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. Estos últimos también existen en el supuesto de que el usuario –ciudadano- entre en contacto con la Administración Pública a través de estas plataformas digitales.

Existen ciertas posibilidades a las que pueden recurrirse para eliminar y, en la medida de lo posible, mitigar estos últimos riesgos que se suscitan en materia de protección de datos. 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. En virtud del fenómeno de la autorregulación resultan posibles los denominados códigos tipo. Si bien los mismos, se han ideado por parte de entidades privadas, también se han creado por la Administración pública. Estas figuras se erigen en sugerentes instrumentos de autorregulación, susceptibles de garantizar la protección de los datos de carácter personal de los ciudadanos en el ámbito digital con carácter general y de las redes sociales con carácter especial.

6. 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.

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, Rafaely 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.

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.

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.
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.
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 UniversitatOberta de Catalunya.
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.
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, Anay 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, Rafaely 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, Jesúsy 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.

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 Serviciosde la Sociedad de la Información y de Comercio Electrónico)*,Madrid, La Ley, pp. 295-307.

RUSSELL, Thomasy 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, Pabloy AREILZA CARVAJAL, José (Coords.), *Internet, una profecía*, Barcelona, Ariel, pp. 15-32.

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

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

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