IMPACTO DE LAS REDES SOCIALES EN EL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES

Esther Mitjans Perelló
Directora de la Agencia Catalana de Protección de Datos de la Generalitat de Cataluña

Resumen: Se ha definido el concepto red social en Internet como un espacio en línea para reforzar las comunicaciones e interrelaciones entre las personas que se registran en ellas, facilitando sus datos personales para configurar un perfil público, en principio visible, para los demás usuarios de la red social. Estos servicios suponen una exposición pública de parte de nuestra vida y van evolucionando hacia nuevas formas de relacionarnos y compartir información y, sin embargo, ni las normas ni nuestra conciencia en materia de privacidad evolucionan al mismo ritmo. Así, es importante identificar los principales conceptos y obligaciones que en materia de protección de datos serian de aplicación a las redes sociales y, por tanto, a los proveedores de estos servicios.

Palabras clave: red social, perfil público, privacidad, seguridad, protección de datos.

Abstract: The concept **social networks** in Internet has been defined as a space online to strengthen Communications and inter-relations between those persons who register their personal data to create a public **profile**, which in principle is visible and accessible to the other users of the social network. These services, which imply publicly exhibiting a part of our lives, have developed new forms of relating with people and sharing information but which have not been accompanied at the same rhythm with the development of regulations nor social consciousness on data protection. Consequently, it is important to identify which principle concepts and obligations of data protection to be applied to social networks, and by extension, to the providers of these services.

Keywords: social networks, public profile, privacy, security, data protection.

SUMARIO: I. EL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES: NUEVOS RIESGOS. II. APLICACIÓN DE LOS PRINCIPIOS DE PROTECCIÓN DE DATOS A LAS REDES SOCIALES. 1. Responsable del fichero o del tratamiento. 2. Datos personales. 3. Derecho de información en la recogida de los datos. 4. Consentimiento para el tratamiento de los datos. 5. Principios de calidad de los datos. 6. Régimen de cesiones de datos personales. 7. Derechos de acceso, rectificación, cancelación y oposición. 8. Medidas de seguridad. III. USOS DE LAS REDES SOCIALES. IV. CONCLUSIONES. BIBLIOGRAFÍA.

I. EL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES: NUEVOS RIESGOS

El derecho a la protección de datos de carácter personal ha surgido a partir de la necesidad de proteger ámbitos de libertad, necesarios para el desarrollo de la personalidad del ser humano, que se han visto amenazados por un posible mal uso de las nuevas tecnologías.

Es un derecho de creación jurisprudencial, pues ha sido el Tribunal Constitucional quien, a partir del artículo 18.4 de la Constitución Española[1] (en adelante, CE) interpretado conforme a los Tratados y Convenios internacionales (artículo 10 CE), ha definido el derecho a la protección de datos de carácter personal entendiéndolo como la posibilidad que tiene toda persona de controlar los datos que se refieren a sí misma.

El Tribunal Constitucional, en la sentencia del Caso Olaverri[2], analizando el artículo 18.4 CE, señala que:

"[...] nuestra Constitución ha incorporado una nueva garantía constitucional, como forma de respuesta a una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona, de forma que en último término no muy diferente a como fueron originándose e incorporándose históricamente los distintos derechos fundamentales. En el presente caso

[1] "La Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".

[2] STC 254/1993, de 20 de junio. Recurso de amparo núm. 1827/1990 (BOE de 18 de agosto de 1993).

estamos ante un instituto de garantía de otros derechos, fundamentalmente el honor y la intimidad, pero también de un instituto que es, en sí mismo, un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de dato [...]" (FJ 4).

En esta primera jurisprudencia reconoce, tímidamente, la existencia de un nuevo derecho que nace como consecuencia de la evolución técnica, aunque no le da el nombre de derecho a la protección de datos de carácter personal, sino que se refiere a él como libertad informática.

Posteriormente, en la sentencia del Caso RENFE[3], el Tribunal Constitucional, en un supuesto en el que los datos sindicales de los trabajadores se habían utilizado para retener parte del salario del recurrente por haber participado, presuntamente, en una huelga (lo cual deducían de su adhesión al sindicato convocante), reitera la doble naturaleza de este derecho: como garantía de otros derechos y como derecho autónomo (libertad frente a posibles agresiones a la dignidad y a la libertad de la persona, provenientes del uso ilegítimo del tratamiento mecanizado de datos)[4]. Según el Tribunal Constitucional: "[...] la libertad informática es así un derecho a controlar el uso de los mismos datos insertos en un programa informático [...]" (FJ 4º).

Si nos fijamos en la evolución legislativa de este derecho, en España la primera norma que lo reguló fue la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de Datos de Carácter Personal. Por el mismo título ya vemos que circunscribía su ámbito de aplicación a los tratamientos de datos personales que se realizaban a través de aplicaciones informáticas.

Posteriormente, la transposición de la Directiva 95/46/CE, del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (en adelante, Di-

[3] STC 11/1998, sentencia de 13 de enero de 1998. Recurso de amparo núm. 2264/1996 (BOE de 12 de febrero de 1998).

[4] El derecho a la autodeterminación informativa se configura como un derecho-garantía, en tanto que es un derecho que por expresa disposición constitucional acompaña a otros derechos para garantizar su ejercicio, pero que, además, están conformados estructural y funcionalmente como verdaderos derechos autónomos (FREIXES SANJUAN y REMOTTI CARBONELL, (1993): 10).

rectiva 95/46/CE) a nuestro ordenamiento interno supone la aprobación de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante, LOPD), que amplía su ámbito de aplicación al conjunto de tratamientos (manuales y automatizados). Así, en su artículo 1 indica que: "La presente Ley Orgánica tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar."

Es esta norma (y las que la desarrollan) la que nos va a servir de hilo conductor para analizar el impacto que las redes sociales tienen en el derecho a la protección de datos personales.

En primer lugar, hemos de definir qué se entiende por dato personal. El Real Decreto 1720/2007, de 21 de diciembre, por el cual se aprueba el Reglamento de desarrollo de la LOPD (en adelante, RLOPD), en el artículo 5 f) define este concepto como: "Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables."

Por tanto, cualquier información que se refiera a nuestra vida, sea un documento, la voz o una fotografía, será considerada como dato personal si permite nuestra identificación.

Otros conceptos que hemos de tener presentes son el de fichero y el de tratamiento de datos, que vienen definidos en el artículo 5 k) y t) del RLOPD como:

"k) Fichero: Todo conjunto organizado de datos de carácter personal, que permita el acceso a los datos con arreglo a criterios determinados, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso."

"t) Tratamiento de datos: cualquier operación o procedimiento técnico, sea o no automatizado, que permita la recogida, grabación, conservación, elaboración, modificación, consulta, utilización, modificación, cancelación, bloqueo o supresión, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias."

Llegados a este punto, veamos a qué nos referiremos al hablar de redes sociales. El concepto de red social no es nuevo, ya que es un ámbito ampliamente estudiado desde la perspectiva de la sociología. Sin embargo, en este artículo me referiré exclusivamente a las redes sociales en Internet, es decir, redes como Facebook, Tuenti, Myspace, etc., ya que es, justamente, el medio –Internet- lo que ha llevado en estos últimos años a

las autoridades de protección de datos a prestarles una especial atención por el fuerte impacto que tienen en el derecho a la protección de datos y por la poca conciencia que, en muchos casos, tienen los usuarios de este impacto. La mayoría de los usuarios tienen la sensación que aquello que hacen en Internet no existe, que no tiene efectos ni consecuencias y que no afectará a su día a día. Sin embargo, todo aquello que hacemos, decimos o mostramos en Internet sigue siendo parte de nuestra vida, parte de nuestra realidad y, por tanto, hemos de activar ciertas precauciones igual que hacemos en el entorno físico.

Las redes sociales en línea pueden definirse como "servicios prestados a través de Internet que permiten a los usuarios generar un perfil público, en el que plasmar datos personales e información de uno mismo y donde disponen de herramientas que permiten interactuar con el resto de usuarios afines o no al perfil publicado"[5].

Nuestra vida se ha tecnificado y, probablemente, ya no podemos imaginar cómo sería ésta sin Internet, sin correo electrónico, etc. Son, por descontado, herramientas muy útiles que la han mejorado, que nos permiten evolucionar en muchos ámbitos y que han modificado la manera de ver nuestro entorno y a las personas que nos "rodean". El concepto de "amigos" usado tradicionalmente ha cambiado en el entorno de las redes sociales en línea, y esto debería llevarnos a ser concientes de qué decimos o dejamos ver a estos amigos del ciberespacio. Los intercambios de información a nivel global son, probablemente, difíciles de medir y, en gran medida, incontrolables. Se han configurado nuevas formas de crear información, de intercambiarla, de acceder a ella. Por otra parte, estas herramientas ya no están sólo en manos de unos pocos, sino que se han popularizado y son utilizadas por todos los niveles sociales, económicos y políticos, y por todos los espectros de edad (tal vez con la excepción de las personas de mayor edad, pese a que cada vez son más las que se acercan a las nuevas tecnologías).

Las redes sociales en Internet se han convertido en lugar de encuentro de miles de personas que, de otra manera, nunca hubieran podido compartir experiencias. Las redes sociales permiten compartir aficiones, ideologías, trabajo, permiten dar respuesta a casi cualquier expectativa.

[5] Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online (2009) Instituto Nacional de Tecnologías de la Comunicación <www.inteco.es> y Agencia Española de Protección de Datos <www.agpd.es >.

Actualmente, se calcula que existen más de 200 redes sociales que ofrecen servicios como perfiles públicos, intercambio de información de todo tipo, actualización automática de la libreta de direcciones, creación de nuevos enlaces y facilitan el acceso a otras aplicaciones, juegos, etc., en línea. En la mayoría de casos se promociona el hecho de que los usuarios inviten a amigos con el fin de ir ampliando la red social. De esta manera, se convierten en importantes plataformas virtuales idóneas por la conexión intensiva y continuada en el tiempo. Todo eso, multiplicado por el amplio número de contactos que se tengan y de las posibilidades de intercambios sociales que se puedan dar.[6]

Existen diferentes tipos de redes sociales atendiendo a sus finalidades: generalistas, temáticas, de relaciones, de contenido, de activismo, profesionales, de ocio... [7]

Las redes sociales son una herramienta de interacción social, en la cual los usuarios comparten sus fotos, vídeos, aficiones, se crean grupos de amigos, blogs...

Las redes generalistas, algunas de las cuales han adquirido gran importancia en los últimos años, disponen de múltiples funcionalidades y herramientas para organizar los contactos, crear grupos, buscar personas, compartir fotografías e incluso desarrollar o usar aplicaciones. Uno de los servicios que ha proporcionado mayor popularidad a las redes es la posibilidad de subir una gran cantidad de fotografías y vídeos. Actualmente, se calcula que el número de fotografías cargadas en Facebook supera los 10.000 millones. Justamente esta utilidad puede generar importantes riesgos para los usuarios a partir del desarrollo de potentes mecanismos de identificación biométrica, como por ejemplo herramientas de reconocimiento facial o, simplemente, a partir del etiquetado de las fotografías por parte de los propios usuarios.

Otra cuestión a tener en cuenta desde la perspectiva de la protección de datos es el tipo de usuarios que utilizan la red social. En un estudio [8] realizado sobre las pautas de uso de las redes sociales, se diferencian dos tipos de perfiles separados por usuarios de 18 a 24 años y usuarios de 25 a 35 años. En cuanto al uso de la red social por parte de estos perfiles, este mismo estudio indica que los usuarios de 18 a 24 años aportan sin mayor problema datos personales, se conectan diariamente, los contactos obtenidos en la propia red son los de más peso y la finalidad principal

[6] <www.wikipedia.com>
[7] <http://socialmedia.lobosuelto.com>, <http://blogs.alianzo.com/redessociales/2009/01/06>
[8] The cocktail analysis <www.tcanalysis.com>

es crear comunidad (pertenecer a la red es un fin en sí mismo). Respecto de los usuarios de 25 a 35 años, encontramos que valoran la seriedad de la red, tienen una actitud más recelosa a la hora de proporcionar datos personales, el círculo laboral suele tener un peso importante, buscan mantener las redes sociales que ya tienen (no hay un interés especial en ampliar el grupo de amigos), la mayoría de los contactos se han generado fuera de la red (offline) y se mantienen en la red (en línea) y están presentes en la red con alguna finalidad: contactos, información, etc. Aunque no debemos desconocer que también hay el tramo de 14 a 17 años que, pese a ser menores de edad, también participan en las redes sociales y de forma masiva. Uno de los problemas que encontramos en este ámbito se refiere a cómo detectar de forma efectiva a los menores y, dentro de ellos, los tramos de edad que conllevan mayor problemática, los menores de 14 años.

Por otra parte, hay un número importante de personas que sin ser usuarios de ninguna red social, en éstas se contiene información relativa a su vida: aparecen en fotografías o vídeos publicados en la red social sin su conocimiento ni consentimiento, se habla de ellos en los foros, blogs, mensajes, etc., o simplemente son destinatarios de invitaciones para formar parte de la red social.

Tanto Internet en general, como las redes sociales en concreto, atraen a un gran número de seguidores y usuarios que se ven beneficiados pero que, también, pueden verse amenazados por los nuevos servicios virtuales de hoy día.

Por otra parte, también ayuda a su gran extensión la facilidad para formar parte de la mayoría de ellas, para lo cual sólo es necesario tener una cuenta de correo electrónico. Esta facilidad que tienen todos los usuarios de Internet para formar parte de una red social e incorporar información de todo tipo, propia y de terceros, genera o requiere cierta reflexión sobre el uso y destino de los datos que circulan por la red social.

A partir de aquí, intentaremos integrar los conceptos y obligaciones que se derivan de la normativa de protección de datos y los elementos que definen una red social, para intentar comprender hasta qué punto la normativa de protección de datos tiene que ser aplicada en este ámbito.

Para ello será de gran ayuda el Dictamen 5/2009 sobre redes sociales en línea, de 12 de junio de 2009 del Grupo del artículo 29. En ella se resuelven algunas dudas acerca de la aplicabilidad de los principios de la Directiva 95/46/CE a las redes sociales. Así, ya en las primeras páginas afirman que muchas de las previsiones de la Directiva 95/46/CE son de

aplicación a los proveedores de servicios de redes sociales (SRS), incluso si están ubicados fuera del Espacio Económico Europeo.

II. APLICACIÓN DE LOS PRINCIPIOS DE PROTECCIÓN DE DATOS A LAS REDES SOCIALES

En nuestro caso, aplicaremos directamente los principios de la LOPD y su normativa de desarrollo al objeto de ir concretando los conceptos, los derechos de los usuarios y las obligaciones de los proveedores de SRS.

No entraremos en el debate sobre la aplicabilidad de la LOPD y su normativa de desarrollo a los proveedores de SRS que operan desde fuera de España. Sin embargo, los principios y obligaciones que se analizarán pueden ser considerados, en su mayoría, como mínimos indispensables para garantizar el derecho a la protección de datos o la privacidad.

1. Responsable del fichero o del tratamiento

Lo primero que debemos determinar es si los proveedores de SRS pueden o no encuadrarse dentro del concepto de responsable del fichero y, por tanto, asumir las obligaciones que la LOPD establece para ellos.

El artículo 5 q) del RLOPD define al responsable del fichero o del tratamiento como la:

"Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que solo o conjuntamente con otros decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente. Podrán ser también responsables del fichero o del tratamiento los entes sin personalidad jurídica".

Así pues, los proveedores de SRS que determinan, en gran medida, la finalidad, el contenido y uso de los datos personales que se incorporan a las redes sociales (pensemos, por ejemplo, en los usos comerciales) encajarían dentro de la definición de responsable del fichero o del tratamiento. No entraremos a analizar el supuesto de los proveedores de aplicaciones, respecto de los cuales el Grupo del artículo 29 ha entendido que en determinados casos también podrán ser considerados como responsables del fichero.

Por otra parte, los tratamientos de datos personales que realizan los usuarios de las redes sociales, en la mayoría de ocasiones, quedarían englobados en la excepción relativa a usos exclusivamente personales o do-

mésticos. Aunque en determinadas circunstancias sí que asumen las obligaciones de un responsable del tratamiento respecto de los tratamientos de datos que realizan, por ejemplo cuando la red social es utilizada por empresas o asociaciones con objetivos comerciales, sociales o políticos. Y, en cualquier caso, cuando los usuarios incorporan información relativa a terceros siguen sometidos a las mismas obligaciones que tendrían en el entorno tradicional.

2. Datos personales

Partiendo de la definición que hemos introducido al principio, no ofrece dudas que la información que se contiene en la red social es, en su mayoría, datos personales, ya que se refieren a personas físicas identificadas o identificables. Por otra parte, tampoco genera duda que nos encontramos ante un tratamiento de información en el sentido del artículo 5 t) del RLOPD; por tanto, la normativa de protección de datos sería aplicable.

En las redes sociales, una vez dado de alta un usuario se le insta a incorporar la mayor cantidad de datos, y lo más precisos posible, y a invitar a otros amigos para que sigan el mismo procedimiento. A partir de aquí el usuario puede delimitar qué quiere que vean los demás de él, qué información quiere compartir. Por tanto, en principio, limitamos "libremente" nuestro derecho a la protección de los datos personales, nuestra intimidad y cualquier otro derecho que pueda verse afectado por el hecho de difundir información relativa a nuestra vida. Sin embargo, hemos de notar que esto no será así en el caso de los datos de terceras personas que puede incorporar el usuario sin haber obtenido su consentimiento, sobre todo en el caso de los datos de personas que no son usuarias de la red social.

¿Qué problemas podemos encontrarnos en las redes sociales? Solamente a título de ejemplo podemos enumerar algunos: riesgos derivados de la publicación de información personal propia o de terceros, suplantación de identidad, acoso, en especial a menores «grooming», comunicaciones comerciales no solicitadas, uso en investigación policial, política, recursos humanos, etc.

Por todo eso, y aunque las redes sociales cuentan con una infinidad de beneficios para sus usuarios, éstos no tienen que obviar el hecho de que se trata de herramientas que permiten la difusión de la información, que la hacen más accesible y utilizable por terceros.

Es cierto que las redes sociales facilitan información y opciones para delimitar y concretar el nivel de acceso o de difusión de la información, es decir, el grado de privacidad. Sin embargo, en general, estas opciones están configuradas por defecto en el nivel más bajo de privacidad, siendo el propio usuario quien debe adaptarlo a sus preferencias. Muchos usuarios, probablemente los más vulnerables, no son concientes de estas posibilidades y de los riesgos que conlleva el no establecer ciertas restricciones respecto a la información que se comparte.

Vista la situación, hay que preguntarse cuál es el nivel de protección legal que tienen los usuarios con respecto a sus datos personales dentro de una red social. El incremento de usuarios cada día es mayor y no existen restricciones en su acceso. Así pues, se pueden incorporar personas de todo tipo, incluidos los menores, entre los que cada día son más populares este tipo de espacios virtuales. Los menores generan una problemática especial, puesto que cada vez son más los que utilizan las redes sociales como medio de relación con las personas de su entorno (familia, colegio, aficiones...), pero también de fuera de su entorno (cuanto más "amigos" tienes, mayor es tu popularidad). Si bien es cierto que se prohíbe el acceso de los menores de edad, por ejemplo, Facebook prohíbe que menores de 13 años se registren y recomienda que los menores de 13 a 18 años pidan permiso a sus padres antes de facilitar información a Facebook, muchos mienten respecto a su edad y los mecanismos de control son bastante limitados y requieren agudizar el ingenio y la imaginación.

En España, el RLOPD establece respecto del tratamiento de datos personales de menores de edad, en su artículo 13, que:

"1. Podrá procederse al tratamiento de los datos de los mayores de catorce años con su consentimiento, salvo en aquellos casos en los que la Ley exija para su prestación la asistencia de los titulares de la patria potestad o tutela. En el caso de los menores de catorce años se requerirá el consentimiento de los padres o tutores.

2. En ningún caso podrán recabarse del menor datos que permitan obtener información sobre los demás miembros del grupo familiar, o sobre las características del mismo, como los datos relativos a la actividad profesional de los progenitores, información económica, datos sociológicos o cualesquiera otros, sin el consentimiento de los titulares de tales datos. No obstante, podrán recabarse los datos de identidad y dirección del padre, madre o tutor con la única finalidad de recabar la autorización prevista en el apartado anterior.

3. Cuando el tratamiento se refiera a datos de menores de edad, la información dirigida a los mismos deberá expresarse en un lenguaje que sea fácilmente comprensible por aquéllos, con expresa indicación de lo dispuesto en este artículo.

4. Corresponderá al responsable del fichero o tratamiento articular los procedimientos que garanticen que se ha comprobado de modo efectivo la edad del menor y la autenticidad del consentimiento prestado en su caso, por los padres, tutores o representantes legales."

Por tanto, si bien a partir de los 14 años los menores pueden consentir respecto del tratamiento de sus datos personales, no podemos olvidar que la manera y el contenido de la información que se les facilite tendrá que ajustarse a su edad. Es particularmente importante tener presente la necesidad de hacerles concientes de bajo qué circunstancias pueden facilitar información de terceras personas.

En este ámbito, debemos mencionar que el Parlamento Europeo ha aprobado un programa comunitario para reforzar la protección de los menores que utilizan Internet, sobre todo los que utilizan redes sociales. Concretamente el programa "Safer Internet", el objetivo del cual es abarcar los temas relacionados con el uso seguro de Internet por parte de los niños y con las nuevas tecnologías en línea. Así, pretende mejorar la protección reduciendo los contenidos ilícitos que se encuentran en la red y llevando a cabo acciones que se anticipen a la manipulación de los menores. El nuevo programa pone en marcha una financiación para proyectos destinados a crear un entorno en línea más seguro para los jóvenes. "Safer Internet" no sólo funciona contra los contenidos ilícitos, sino también perjudiciales. Los fondos económicos también servirán para "desarrollar los conocimientos especializados sobre los usos existentes y emergentes, los riesgos y las consecuencias de las tecnologías en línea para la vida de los niños, incluidos los aspectos técnicos, aspectos psicológicos y sociológicos relacionados con la línea de abuso sexual infantil"[9].

En el ámbito de los menores y adolescentes es destacable el Memorándum de Montevideo[10], en el cual se dan una serie de recomendaciones a los Estados en materia legal, de políticas públicas y a la industria, haciendo especial hincapié en la necesidad de educar tanto a los padres

[9] COMISIÓN EUROPEA (2009)

[10] Memorándum sobre la protección de datos personales y la vida privada en las redes sociales en Internet, en particular de niños, niñas y adolescentes. Reunión de consulta para la redacción de recomendaciones sobre protección de datos y vida privada, en particular de niños, niñas y adolescentes en las redes sociales en Internet, Montevideo, 27 y 28 de julio de 2009.

y tutores como a los menores y adolescentes para un uso responsable de Internet y de las redes sociales en línea. Es necesario trabajar las capacidades de padres, tutores y menores en el uso de las tecnologías de la comunicación, con el fin de que puedan aprovecharse de los máximos beneficios que ofrecen estos instrumentos para su propio desarrollo como personas pero, también, que sean capaces de gestionar de manera efectiva los riesgos y amenazas que pueden encontrarse.

3. Derecho de información en la recogida de los datos

Según se establece en el artículo 5 de la LOPD, en el momento de la recogida de los datos debemos ser informados de modo expreso, preciso e inequívoco:

De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.

Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.

De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.

De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.

De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

En el caso de utilizar cuestionarios o formularios, la información arriba indicada debe constar de forma claramente legible. Así, el conjunto de la información debería constar de forma evidente en el momento de registrarse en una red social.

Por otra parte, si los datos personales que recogemos y tratamos en nuestros sistemas de información no han sido recogidos directamente de la persona interesada, también debemos informarle de los extremos antes mencionados, así como del contenido del tratamiento y de la procedencia de los datos, dentro de los tres meses siguientes al momento del registro de los datos, salvo que ya hubiera sido informado con anterioridad[11]. Así, algunos proveedores de SRS no sólo tratan la información

[11] El artículo 5.5 de la LOPD establece una serie de excepciones en este caso: "No será de aplicación lo dispuesto en el apartado anterior cuando expresamente una Ley lo prevea, cuando el tratamiento tenga fines históricos, estadísticos o científicos, o cuando la información al interesado resulte imposible o exija

que las personas facilitan en el momento de registrarse, sino que además buscan más información en la propia red social y fuera de ella.Asimismo, como se indica en el Memorándum de Roma[12], no sólo es importante la transparencia en el momento de registrarse respecto de los tratamientos de datos que se llevarán a cabo, sino que en este ámbito es especialmente importante recordar los riesgos que el usuario asume al incorporar datos personales propios y de terceros en la red social. A esto añade la importancia de informar sobre estas cuestiones de manera dinámica durante el uso del servicio, en función de las diferentes acciones que el usuario va llevando a cabo.

Más allá de los términos del artículo 5 de la LOPD, es importante que los proveedores de SRS asuman obligaciones en cuanto a la formación e información de sus usuarios y desarrollen políticas informativas que les ayuden a navegar de forma más segura por la red social en línea. Así, por ejemplo, respecto a los beneficios de usar seudónimos, a entender las alertas de seguridad, a conocer las responsabilidades que pueden derivarse de sus acciones, a cómo ejercer sus derechos... Las políticas de privacidad cobran importancia en un ámbito donde la formación y la conciencia del riesgo suelen ser escasos por no decir inexistentes.

4. Consentimiento para el tratamiento de los datos

Cuestión aparte es determinar si es o no necesaria la obtención del consentimiento del titular de los datos[13]. En este caso, deberíamos diferenciar los datos de los usuarios que sean estrictamente necesarios para

esfuerzos desproporcionados, a criterio de la Agencia de Protección de Datos o del organismo autonómico equivalente, en consideración al número de interesados, a la antigüedad de los datos y a las posibles medidas compensatorias.

Asimismo, tampoco regirá lo dispuesto en el apartado anterior cuando los datos procedan de fuentes accesibles al público y se destinen a la actividad de publicidad o prospección comercial, en cuyo caso, en cada comunicación que se dirija al interesado se le informará del origen de los datos y de la identidad del responsable del tratamiento así como de los derechos que le asisten.

[12] International Working Group on Data Protection in Telecommunications: *Report and Guidance on Privacy in Social Network Services –Rome Memorandum-*, 3-4 March 2008.

[13] Artículo 6 de la LOPD. Consentimiento del afectado

"1. El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa.

2. No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7 apartado 6 de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción

la prestación del servicio o servicios solicitados y el consentimiento para el tratamiento de información que no esté vinculada directamente a la prestación del servicio (por ejemplo, actuaciones comerciales o de *marketing*). En el primer caso, no sería necesario el consentimiento del titular de los datos, pero sí en el segundo caso. En este segundo supuesto debería darse la posibilidad al titular de los datos de manifestar, de forma sencilla y rápida, su negativa a los tratamientos no necesarios para la prestación del servicio. Sería recomendable dar esta opción en el mismo momento en que se facilita el derecho de información cuando se produce la recogida de los datos. Sin embargo, me parece interesante la apreciación de la Comisaria para la protección de la vida privada de Canadá, que en un caso contra Facebook[14] indica que los usuarios no pueden denegar el consentimiento a cualquier forma de publicidad ya que, al ser la red social un servicio gratuito, requiere para su mantenimiento alguna forma de publicidad. Sin embargo, recuerda que sí debe permitirse denegar el consentimiento en el caso de la publicidad social al ser ésta más invasiva. En este punto, Facebook ha aceptado ser más claro en la descripción de la publicidad y facilitar a los usuarios la localización de la información relativa a este tema.

No podemos olvidar que tanto en el momento del registro como posteriormente se puede incorporar información relativa a la salud, orientación sexual, opiniones políticas, ideología y que este tipo de información está especialmente protegida por la normativa de protección de datos al referirse a aspectos muy íntimos de la persona. En este caso el consentimiento expreso e informado cobra especial importancia.

Por otra parte, continua siendo necesario reflexionar sobre la necesidad de obtener el consentimiento para el tratamiento de datos de aquellas personas que no son usuarias de la red social: ¿quién debe obtenerlo?, ¿en qué momento? En este caso, el Grupo del artículo 29 entiende que el tratamiento de los datos de no usuarios sólo puede realizarse por el

---

del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado.

3. El consentimiento a que se refiere el artículo podrá ser revocado cuando exista causa justificada para ello y no se le atribuyan efectos retroactivos.

4. En los casos en los que no sea necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal, y siempre que una Ley no disponga lo contrario, éste podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En tal supuesto, el responsable del fichero excluirá del tratamiento los datos relativos al afectado.

[14] Rapport de conclusions de l'enquête menée à la suite de la plainte déposée par la Clinique d'Intêret Public et de Politique d'Internet du Canada contre Facebook INC. aux termes de la Loi sur la protection des renseignements personnels et les documents électroniques, 16 juillet de 2009.

proveedor de SRS si se cumple con alguno de los supuestos establecidos en el artículo 7 de la Directiva 95/46/CE[15]. En todo caso, pensemos que en España, incluso en aquellos supuestos en que no es necesario el consentimiento, sigue siendo obligatorio facilitar el derecho de información excepto en contadas ocasiones[16].

Por otra parte, en el caso contra Facebook la Comisaria para la protección de la vida privada de Canadá entiende que la acción de subir información de personas no usuarias en los muros o en los perfiles se realiza con fines puramente personales y, por tanto, no debe aplicarse la normativa de protección de datos. En el caso del etiquetaje de fotos (en este caso se puede incluso etiquetar con una dirección de correo electrónico) y de las invitaciones enviadas a los no usuarios, Facebook debería cumplir la normativa de protección de datos si utiliza los datos para sus propios fines. Entiende la Comisaria que puede establecerse que sean los propios usuarios los que deben obtener el consentimiento de los terceros, aunque correspondería al proveedor de SRS, con una diligencia razonable, garantizar que los usuarios saben que tienen esta obligación antes de comunicar la dirección de correo electrónico a Facebook y sancionar a aquellos que no respeten esta obligación. En este ámbito, recomienda al proveedor que mejore el servicio de invitación y que establezca un límite temporal razonable para la conservación de las direcciones de correo de los no usuarios.

5. Principios de calidad de los datos

En el artículo 4 de la LOPD se establece que los datos personales:

[15] Artículo 7 de la Directiva 95/46/CE: Los Estados miembros dispondrán que el tratamiento de datos personales sólo pueda efectuarse si:

a) el interesado ha dado su consentimiento de forma inequívoca,

b) es necesario para la ejecución de un contrato en el que el interesado sea parte o para la aplicación de medidas precontractuales adoptadas a petición del interesado, o

c) es necesario para el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento,

d) o es necesario para proteger el interés vital del interesado, o

e) es necesario para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento o a un tercero a quien se comuniquen los datos, o

f) es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales

[16] Artículo 5.5 y 24.1 de la LOPD

Deberán ser adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.

No podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos.

Deberán ser exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado. Aquellos datos que sean inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio.

Deberán ser cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados. No pueden conservarse de forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados.

Estos principios establecen una serie de obligaciones para el responsable del fichero o del tratamiento que, en el caso de las redes sociales, exige diferenciar los datos necesarios para el registro, los datos que el proveedor del servicio puede obtener de otras fuentes, los datos propios y de terceros que incorporan los propios usuarios.

Alguno de estos principios pueden ser más sencillos de aplicar por el proveedor de SRS respecto de los datos incorporados en el momento del registro. Por ejemplo, el principio de calidad de los datos en cuanto uso de los datos sólo para las finalidades del servicio o respecto de aquellas que el usuario ha consentido, cancelación de los datos que no sean ya necesarios para la finalidad que motivó la recogida. Otros principios u obligaciones, por el contrario, pueden comportar mayor dificultad de aplicación que, pongamos por ejemplo, el de mantener los datos exactos y puestos al día (aunque en este caso el propio RLOPD incorpora elementos en este aspecto en el artículo 8.5, en que establece que si los datos han sido recogidos directamente del afectado, se considerarán exactos los facilitados por éste). Por tanto, el problema se encontraría en los datos no facilitados por el interesado sino por otro usuario, o los datos obtenidos por el proveedor del servicio de otras fuentes.

6. Régimen de cesiones de datos personales

La cesión de datos personales plantea ciertas particularidades, o más bien exige mayores garantías, puesto que supone para su titular una importante perdida de control sobre los datos personales cedidos. Por tan-

to, derechos como el de información o el principio del consentimiento informado cobran especial trascendencia en este ámbito.

En este supuesto, cuando el responsable del tratamiento desee comunicar datos a terceros, tanto entidades privadas como administraciones públicas, debería obtener el consentimiento previo del titular de los datos o, en su caso, existir una norma con rango legal que habilite la comunicación de los datos personales[17].

Especial atención merecen los proveedores de aplicaciones para las redes sociales en línea. El proveedor de SRS debe adoptar actitudes diligentes respecto a: limitar el acceso a datos personales por parte de los proveedores de aplicaciones, por ejemplo indicar con precisión que sólo deben recoger aquellos datos que sean estrictamente necesarios para poder utilizar la aplicación; advertirles de la necesidad de obtener el consentimiento informado cuando quieran tratar datos personales de los usuarios más allá de los estrictamente necesarios; mantener una política informativa clara y accesible, es decir, establecer garantías para que los usuarios de estas aplicaciones sean concientes del uso de sus datos personales y puedan decidir sobre éste.

7. Derechos de acceso, rectificación, cancelación y oposición

No entraremos en el análisis individualizado de estos derechos, simplemente constataremos que en el caso de las redes sociales también están vigentes y, por tanto, deberán ser atendidos por el responsable del tratamiento tanto respecto de los datos de los usuarios de las redes sociales como respecto de los no usuarios.

En el caso del derecho de acceso, creo conveniente recordar (ya que en muchas ocasiones no se tiene en cuenta) que no sólo permite conocer

17 El artículo 11 de la LOPD, en su apartado 2, establece otras excepciones al consentimiento, como por ejemplo: cuando se trate de datos recogidos de fuentes accesibles al público, cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. En este caso, la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique, cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas. Tampoco será preciso el consentimiento cuando la comunicación tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas, cuando la cesión se produzca entre Administraciones Públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos, cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica.

qué datos tiene el responsable del fichero sino también el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos.

Por otra parte, es plenamente aplicable el derecho de cancelación. Aunque hemos de tener en cuenta que uno de los riesgos que se predican de Internet, y de las redes sociales en concreto, es que en ellas no existe el olvido, puesto que aunque nosotros eliminemos nuestra información o lo haga el proveedor de SRS, no podemos controlar quien lo ha copiado desde el lugar de origen ni que usos puede darle.

Es importante que se establezcan mecanismos fáciles de utilizar y de encontrar en el entorno para facilitar el ejercicio de los derechos ARCO.

En el caso contra Facebook[18] mencionado anteriormente se recomendaba que los datos de los usuarios que han desactivado sus cuentas fueran suprimidos pasado un periodo razonable y, en todo caso, que se informara a los usuarios.

8. Medidas de seguridad

La seguridad de la información es un elemento imprescindible para mantener la confianza de los usuarios en las redes sociales. Los proveedores de SRS deben adoptar todas las medidas técnicas, legales y organizativas necesarias para asegurar el correcto uso de la información contenida en la red social. En éste ámbito, las medidas preventivas cobran especial importancia para evitar el tratamiento no autorizado de datos de carácter personal. Una vez difundida la información personal, es difícil (diría imposible) restaurar el derecho a la protección de datos personales. Es importante centrar los esfuerzos en evitar accesos no autorizados, fraudes...

Como indica el Grupo de trabajo de Protección de Datos en las Telecomunicaciones[19] en su trabajo sobre las contingencias de la privacidad y la seguridad, el riesgo de filtraciones de información siempre está latente y será difícil conseguir una seguridad absoluta. Aún así, si se empieza por bloquear las aplicaciones dañinas que se agregan a las redes sociales que suponen una amenaza adicional y, por otra parte, se siguen creando me-

[18] Rapport de conclusions de l'enquête menée à la suite de la plainte déposée par la Clinique d'Intêret Public et de Politique d'Internet du Canada contre Facebook INC. aux termes de la Loi sur la protection des renseignements personnels et les documents électroniques, 16 juillet de 2009.

[19] International Working Group on Data Protection in Telecommunications (2008)

didas restrictivas del acceso y eliminando la posibilidad de llegar al perfil de los usuarios mediante los motores de búsqueda y aplicaciones tanto internas como externas, puede mejorar en gran medida el nivel de seguridad de las redes sociales.

III. USOS DE LAS REDES SOCIALES

Las redes sociales que originariamente se han utilizado como punto de encuentro entre amigos, para buscar personas del pasado, para el ocio y el entretenimiento, para compartir en definitiva experiencias, han ido avanzando hacia nuevos usos que deben ser tenidos en cuenta por los usuarios. Así, por ejemplo, las empresas las están utilizando para conocer facetas de sus trabajadores a las cuales de otra manera no podrían tener acceso. También para conocer el perfil de los candidatos a un puesto de trabajo, la información personal podría llegar a determinar si una persona es o no apta para un puesto de trabajo. En algunos casos son utilizados por los *headhunters* para localizar candidatos de alto nivel. Recientemente, se han publicado algunas noticias[20] que indican que el 13,3% de las empresas españolas reconoce que busca información en Internet sobre posibles candidatos. Esta práctica puede llevar a perder o conseguir un trabajo según los contenidos que allí figuren. Las administraciones públicas también están explorando el uso de las redes sociales como mecanismo para acercarse a los ciudadanos.

Otro de los nuevos usos que se le están dando en las redes sociales es el de difusión y promoción de partidos políticos. Éstos han encontrado en las redes sociales una plataforma para llegar, también, a los más jóvenes. Es un sistema fácil de usar y gratuito que les permite darse a conocer. Además, les permite ponerse en contacto con sus usuarios para convocarlos o informarlos de las novedades que presentan.

También, en el sector comercial, las redes están adquiriendo protagonismo y los proveedores de SRS están adaptándose a las necesidades de estos nuevos usuarios. Así, aparecen redes sociales para profesionales que permiten una comunicación fluida y el intercambio de experiencias. En definitiva, es una nueva manera de hacer contactos y realizar negocios en Internet.

[20] <www.noticiasfacebook.com> (2009)

IV. CONCLUSIONES

Las redes sociales en Internet han abierto un nuevo campo de expansión personal para todos sus usuarios, aportan enormes beneficios y pueden ser instrumentos de desarrollo personal, sin embargo, como cualquier otro entorno, puede comportar riesgos para aquellos que se incorporan a ellas sin tener elementos que les permitan identificar las amenazas y, por tanto, prevenirlas.

La idea que muchas personas tienen respecto a que Internet es un mundo anónimo, que lo que hacemos, decimos, mostramos en Internet, en una red social, no tiene consecuencias para nuestra realidad física, nos lleva a ser descuidados en aspectos de nuestra vida que en otro entorno tendríamos fuertemente resguardados. Al registrarse en una red social los usuarios facilitan gran número de datos personales, desde datos identificativos básicos a datos que, bien directamente o bien a través de la deducción, pueden dar información sobre aspectos muy sensibles, como puede ser nuestro estado de salud, nuestra orientación sexual, nuestras opiniones políticas o nuestra religión.

Las redes sociales incorporan instrumentos que, en mayor o menor medida, pueden servirnos para proteger nuestra privacidad. Aunque en la mayoría de ocasiones el nivel de privacidad que viene configurando por defecto es el menor y, por tanto, deben ser los usuarios quienes deben adaptarlo a sus preferencias. Sin embargo, la correcta adaptación a las preferencias de cualquier persona presupone que esa persona conoce y comprende las diferentes posibilidades y las consecuencias de elegir unas u otras y, en éste ámbito, el desconocimiento del riesgo es lo que marca, en gran medida, la actuación de los usuarios.

Otra problemática que surge es la gran acogida que han tenido algunas redes sociales entre los menores de edad. Seguramente podemos afirmar que están sometidos a los mismos riesgos y amenazas pero, en todo caso, son un colectivo más vulnerable frente a cualquier acción malintencionada por parte de otros usuarios de la red social.

En este trabajo se han intentado identificar, a partir de la normativa de protección de datos española, las principales obligaciones de un proveedor de SRS en esta materia, sin tener en cuenta el aspecto de la territorialidad. Principios como los de calidad de los datos, de información, de consentimiento, de seguridad, etc., son los mínimos que deberían regir cualquier tratamiento de datos de carácter person-

al. Pero todos ellos en el marco de las redes sociales tienen particularidades, por ejemplo cómo determinar cuáles son los datos estrictamente necesarios para la prestación de un servicio que, justamente, consiste en facilitar al usuario una plataforma para compartir con los demás la mayor cantidad de información posible. O el principio de información, que en este ámbito probablemente deba ir más allá de informar sobre el concreto tratamiento de la información que se realice, tanto de forma visible como invisible, e informar dinámicamente sobre los riesgos inherentes a la divulgación de la información personal en Internet y cómo protegerse frente a ellos. En el caso del consentimiento recordar la problemática que hemos indicado sobre los datos de las personas no usuarias de las cuales se incorpora información en la red social.

Es imprescindible que tanto los Estados como los proveedores de servicios asuman un papel activo en este nuevo entorno. La formación y la información respecto a cómo usar con garantías las redes sociales requiere de una actuación conjunta y coordinada para proteger a los usuarios, pero particularmente aquellos segmentos más vulnerables como los menores. Deben darse instrumentos para que todos los usuarios sean capaces de gestionar sus propios riesgos en los nuevos entornos que proporcionan las nuevas tecnologías.

BIBLIOGRAFIA

COMISSIÓN EUROPEA (2009): *Safer Internet Programme 2009-2013*

FREIXES SANJUAN, Teresa, y REMOTTI CARBONELL, José Carlos (1993): *El derecho a la libertad personal*, Barcelona, Ed. PPU, pág. 10

THE COCKTAIL ANALYSIS, 18 de noviembre de 2008: Herramienta de comunicación on-line: Las Redes Sociales

INTERNATIONAL WORKING GROUP ON DATA PROTECTION IN TELECOMMUNICATIONS (3-4 March 2008): *Report and Guidance on Privacy in Social Network Services*, "*Rome Memorandum*"

NORMATIVA

Constitución Española de 1978

Dictamen 5/2009 sobre redes sociales en línea de 12 de junio de 2009 del Grupo del artículo 29

Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24/10/1995, 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.(Diario Oficial núm. L 281, de 23/11/1995)

Ley Orgánica 5/1992, de 29 de octubre, de regulación del Tratamiento Automatizado de Datos de Carácter Personal

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

Memorándum sobre la protección de datos personales y la vida privada en las redes sociales en Internet en particular de niños, niñas y adolescentes. Reunión de consulta para la redacción de recomendaciones sobre protección de datos y vida privada, en particular de niños, niñas y adolescentes en las redes sociales en Internet, Montevideo, 27 y 28 de julio de 2009.

Raport de conclusions de l'enquête menée à la suite de la plainte déposée par la Clinique d'IntêretPublic et de Politique d'Internet du Canada contre Faceebool INC. aux termes de la Loi sur la protection des renseignements personnels et les documents électroniques, 16 de julio de 2009.

Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

JURISPRUDENCIA

STC 254/1993, de 20 de junio. Recurso de amparo núm. 1827/1990 (BOE de 18 de agosto de 1993).

STC 11/1998, sentencia de 13 de enero de 1998. Recurso de amparo núm. 2264/1996 (BOE de 12 de febrero de 1998).

WEBGRAFIA

"Red Social", "Facebook" www.wikipedia.org

THE COCKTAIL ANALYSIS : "Observatorio sobre la evolución de las redes sociales" http://tcanalysis.com

Instituto Nacional de Tecnologías de la Comunicación: "Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online" (2009) www.inteco.es

Agencia Española de Protección de Datos www.agpd.es

http://socialmedia.lobosuelto.com

http://blogs.alianzo.com/redessociales/2009/01/06

www.noticiasfacebook.com (2009)