

REFLEXIONES JURIDICAS EN TORNO A LAS REDES SOCIALES Y SU TRASFONDO ECONÓMICO

Carmen Casado

Asociado. Responsable del Departamento de Tecnologías de la Información y Comunicación. JAUSAS

1. INTRODUCCIÓN
2. PRINCIPALES RIESGOS EN MATERIA DE PROTECCIÓN DE DATOS Y PRIVACIDAD
3. MARCO REGULADOR E INICIATIVAS LEGISLATIVAS
4. CONCLUSIONES

I. INTRODUCCIÓN

Internet y la llegada de la banda ancha han supuesto una auténtica revolución en nuestra sociedad. Buena prueba de ello es el arrollador fenómeno de las redes sociales y el incesante protagonismo que éstas han ido adquiriendo durante los últimos años, transformando nuestra forma de relacionarnos, comunicarnos, divertirnos e incluso buscar trabajo, lo que ha dado lugar, a su vez, a la aparición de nuevos modelos de explotación económica.

Gracias a la cantidad de datos que manejan, estas redes sociales se han convertido en una herramienta de marketing muy poderosa para las empresas a la hora de promocionar sus productos, ganando cada vez más terreno a los tradicionales métodos de publicidad. Éstos ya no pueden competir en coste y velocidad de difusión con las nuevas alternativas publicitarias como la publicidad contextual o relacional y el marketing viral.¹

Existen infinidad de tipos de redes sociales: de perfil profesional, de ocio, de intercambio de contenidos, enfocadas a colectivos particulares o a determinadas aficiones (música, cine o arte). Incluso comienza a ser práctica extendida entre las empresas, para promocionar sus productos, el crear comunidades virtuales de usuarios en las que sus clientes pueden interactuar y compartir sus experiencias respecto al uso y consumo de sus productos.

¹ Publicidad contextual: en función del análisis del perfil del usuario, la red social dirigirá al usuario publicidad personalizada, basada en sus gustos, inquietudes, preferencias, y páginas visitadas.

Marketing viral: técnica de marketing utilizada para producir incrementos exponenciales en “crecimiento de marca”, mediante procesos de autorreplicación viral análogos a la expansión de un virus informático. Ejemplos de marketing viral, “amo a Laura” o la campaña de Rodolfo Chikilicuatre (Fuente: Wikipedia).

De todas ellas, las más extendidas y las que entrañan además mayores riesgos para la privacidad son las redes de ocio, por el volumen de información que procesan, ya que el modelo de negocio está basado en la voluntad del usuario de proporcionar y compartir información sobre su persona, costumbres, gustos y aficiones. Un auténtico escaparate virtual en el que el control de la información es muy limitado pues, una vez facilitada la misma, se desconoce dónde, cuándo y por quién puede ser vista y utilizada, con qué fines y durante cuánto tiempo. Ello es especialmente relevante en el caso de menores.

Asimismo, al ser un fenómeno de difusión mundial en constante y creciente desarrollo, carecemos en la actualidad de un marco jurídico normativo uniforme que nos proporcione seguridad jurídica, así como unos criterios de actuación frente a eventuales problemas, riesgos o conflictos que el uso de tales plataformas puede comportar.

II. MARCO REGULADOR E INICIATIVAS LEGISLATIVAS A NIVEL EUROPEO

En Europa disponemos de un amplio marco jurídico pues, además de contar con varias directivas que regulan aspectos relativos a la protección de datos de carácter personal y su seguridad en el ámbito de las telecomunicaciones,² la Comisión Europea, consciente de las nuevas tendencias de la economía digital adoptó, en noviembre de 2007, una Propuesta de Directiva para modificar, entre otras normas, la Directiva 2002/58/CE relativa al Tratamiento de los Datos Personales y a la Protección de la Intimidad en el Sector de las Telecomunicaciones y el Reglamento (CE) nº 2006/2004, sobre la cooperación en materia de consumidores.

Dicha Propuesta de Directiva, aún pendiente de aprobación definitiva, recoge, entre otras muchas medidas, la aplicación de la legislación europea en materia de protección de datos y privacidad en el sector de las telecomunicaciones a las redes privadas de comunicación (redes sociales), lo que supone un importante avance en la materia, abonando asimismo el terreno hacia los nuevos retos que presenta el mercado digital.

También hemos de destacar la iniciativa de la Comisión al publicar, en septiembre de 2008, una Comunicación sobre las Redes y la Internet del Futuro, en la que expone los desafíos que las nuevas tendencias supondrán para la economía digital, a la vista de la interoperabilidad y la convergencia de los medios digitales.

² A destacar, la Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección de las personas físicas en lo que respecta al Tratamiento de Datos Personales y a la Libre Circulación de estos datos, y la Directiva 2002/58/CE, relativa al Tratamiento de los Datos Personales y a la Protección de la Intimidad en el Sector de las Telecomunicaciones.

Por otro lado, el Grupo de Trabajo del Artículo 29 ³ también mantiene una activa labor en este sentido, pues además de haber emitido distintas opiniones sobre la propuesta de modificación de la Directiva 2002/58/CE (la última de ellas el pasado 10 de febrero de 2009, Opinión 2/2008), ha publicado otros documentos en los que trata particularmente la problemática de las redes sociales (“Rome Memorandum, Report and Guidance on Privacy in Social Network Services”, Marzo de 2008), proporcionando información sobre los riesgos de su utilización y efectuando recomendaciones a los usuarios de las mismas.

De igual forma, la Agencia Europea de Seguridad de las Redes y de la Información (ENISA) ha publicado diversos documentos, entre ellos, unas recomendaciones sobre la seguridad en las redes sociales online (“Security Issues and Recommendations for Online Social Networks”, octubre de 2007), en las que analiza cómo los problemas de seguridad aún no resueltos de la propia Internet pueden, a su vez, acentuar el riesgo en el uso de las redes sociales (virus, gusanos, *phishing* específico de redes sociales, espionaje corporativo, *inter alia*).

Pero pese a todo ello, el principal obstáculo ante el que nos encontramos es que numerosas redes sociales operan desde fuera de la Unión Europea (y muchas de ellas desde Estados Unidos), por lo que la normativa comunitaria puede no resultar de aplicación⁴. Del mismo modo, la estadounidense se segmenta en un entramado legislativo estatal y federal, de carácter sectorial, complejo de desgranar, lo que aporta indudablemente mayor complejidad.

De ahí que por parte de los diversos países se promueva la autorregulación del sector con distintas iniciativas, tanto a nivel público como privado, con el objetivo de informar a los sujetos involucrados en las redes de cómo han de utilizar tales plataformas y de los riesgos a los que pueden estar expuestos.

En este sentido, las autoridades europeas en materia de protección de datos tienen prevista una Conferencia en Madrid, el próximo mes de noviembre, en la que tratarán, entre otras materias, la importancia de la seguridad en las redes sociales, abordando incluso la posible redacción de un Tratado Internacional de Protección de Datos Personales, que permita disponer de una regulación extraterritorial que se adecue a las características propias de este tipo de servicios.⁵

³ Órgano consultivo independiente de la UE, creado por el artículo 29 de la Directiva 46/95/CE, para la protección de las personas en lo que respecta al tratamiento de datos personales. Entre sus funciones está el asesorar a la Comisión así como elaborar dictámenes y recomendaciones en materia de protección de datos.

⁴ A título orientativo, *vide* Documento de trabajo del Grupo del Artículo 29, de mayo de 2002, (WP56), relativo a la aplicación internacional de la legislación comunitaria sobre protección de datos al tratamiento de los datos personales en Internet por sitios Web establecidos fuera de la UE.

⁵ Estudio sobre la Privacidad de los Datos Personales y la Seguridad de la Información en las Redes Sociales, AEPD e INTECO, Febrero 2009.

III. REFLEXIONES JURÍDICAS EN MATERIA DE PROTECCIÓN DE DATOS Y PRIVACIDAD

Todo este entramado jurídico en constante evolución nos presenta como juristas numerosos retos. Ante estos nuevos escenarios, ¿nos valen los métodos tradicionales del Derecho para resolver los problemas que desata el uso de tales mecanismos?

El pasado 12 de Febrero la Agencia Española de Protección de Datos (AEPD), en conjunción con el Instituto Nacional de Tecnologías de Comunicación (INTECO), publicó un Estudio sobre la Privacidad de los Datos Personales y la Seguridad de la Información en las Redes Sociales. Según dicho estudio, el 43% de los usuarios tiene configurado su perfil de forma que puede ser visto por cualquier persona. Dicha afirmación nos conduce a una serie de reflexiones:

1. ¿Es realmente el usuario de tales redes sociales consciente de que cuando accede a tales servicios está “suscribiendo” un contrato, contratando un servicio y pagando un precio por ello?
2. ¿Conoce efectivamente los términos y condiciones en los que se le va a prestar dicho servicio? ¿Se lee previamente las condiciones de uso y privacidad de la plataforma como si de un contrato se tratase?
3. ¿Podemos afirmar que verdaderamente confluye un consentimiento informado por parte del usuario? ¿Y del usuario menor de edad?
4. ¿Es realmente consciente del “precio” que está abonando? Porque detrás de ese velo de gratuidad aparente en la prestación del servicio existe un precio, y éste viene conformado por la cantidad de datos personales y usos de los mismos que el usuario permite realizar a la empresa titular de la plataforma, a través de la configuración de su perfil de privacidad.

Es la entrega de ese “precio” lo que puede comportar serios riesgos legales en materia de protección de datos y privacidad, a destacar ⁶:

- El usuario puede estar proporcionando más información sobre sí mismo y los demás de la que inicialmente cree. A título de ejemplo, existe en el mercado software de reconocimiento facial que puede ser empleado

⁶ Extracto del Estudio sobre la Privacidad de los Datos Personales y la Seguridad de la Información en las Redes Sociales, publicado por la AEPD e INTECO, en Febrero 2009, así como del “Rome Memorandum”, Documento elaborado por el Grupo de Trabajo del Artículo 29, publicado el pasado 4 de marzo de 2008.

para recabar datos biométricos del usuario o de terceros a los que éste que haya “etiquetado” en una fotografía.

- También se puede poner en riesgo la privacidad de terceros al publicar información sobre los mismos que sea falsa o que, aún siendo verdadera, su difusión no haya sido consentida por sus titulares.
 - Es probable que puedan producirse accesos incontrolados al perfil de un usuario, ya que cualquier otro usuario puede generalmente acceder a la información y disponer de la misma a su antojo (copiarla, almacenarla o reenviarla).
 - La información publicada puede aparecer indexada en los buscadores de Internet, lo que vendría a dificultar su futura eliminación aunque el usuario se hubiera dado de baja del servicio. Es el denominado “Hotel California Effect” (*you can check out, but you can never leave*).⁷
 - Riesgos de suplantación de identidad en la Red, *spam*, *phishing* o *pharming*.
 - Dificultades a la hora de obtener la baja del servicio así como desconocimiento del tiempo durante el cual la plataforma conservará la información proporcionada.
 - Instalación y uso de *cookies* sin conocimiento del usuario, lo que permitiría conocer el lugar desde donde el usuario accede, el tiempo que éste permanece conectado, los sitios que visita y los clics que efectúa.
 - Utilización de *Web beacons*, imágenes electrónicas incluidas en correos electrónicos o anuncios que permiten conocer el contenido online visitado por el usuario.
 - Recepción de publicidad hipercontextualizada, esto es, publicidad personalizada dirigida al usuario basada en el previo análisis de sus gustos, inquietudes, preferencias.
5. Es el usuario quien, en principio, libre y voluntariamente, publica y difunde sus datos de carácter personal en la red social, lo que legitima a las mismas a realizar los usos que estimen convenientes. ¿Estaría ello transformando a estas plataformas en auténticos “paraísos cibernéticos” que exoneran su responsabilidad trasladándola directamente al usuario?
6. ¿De qué herramientas disponemos cuando la plataforma, de forma unilateral, modifica sustancialmente las condiciones del contrato y/o impone en las mismas cláusulas abusivas? ¿Qué podemos hacer ante un caso como el recientemente vivido por los usuarios de Facebook, en el que la

⁷ Fack Sheet “ Social Networking Sites”, ENISA 2008.

plataforma modificó subrepticamente su política de confidencialidad, con la finalidad de reservarse el derecho de utilizar los datos generados por el usuario a perpetuidad, incluso la información ya borrada? ¿Qué tipo de consentimiento sería necesario por parte del usuario para entender efectivamente novado el contrato?

III. CONCLUSIÓN

Confiamos en que las iniciativas legislativas en curso y las numerosas recomendaciones, guías de uso y códigos de conducta promovidas, tanto a iniciativa pública como privada, por los distintos países, nos ayuden sobre todo a conocer y maximizar las ventajas que el uso de tales plataformas de comunicación y sus múltiples utilidades nos pueden reportar como usuarios, al tiempo de que nos permitan minimizar los riesgos legales que su uso ilegítimo o inadecuado puede llevar aparejado ya que, en última instancia, como usuarios, somos responsables de nuestros datos.

En cualquier caso, aunque la armonización legislativa tarde en producirse, el propio mercado va aportando “soluciones” a los abusos que detecta: véase si no la presión ejercitada por los cincuenta mil usuarios de Facebook frente a la modificación arbitraria de su política de confidencialidad: en unos pocos días consiguieron que la Plataforma restaurara su anterior clausulado. Ello no es más que otro ejemplo de la fuerza, alcance y difusión del denominado fenómeno “viral”.