

PROTECCIÓN DE DATOS PERSONALES EN EL DERECHO EUROPEO.

E-PRIVACIDAD EN LAS REDES SOCIALES

Parece paradójico que en una sociedad como la nuestra marcada por un fuerte individualismo uno de los temas que mayor interés despierte es la participación social y como se instrumentaliza.

El contexto de la comunicación social ha cambiado a gran velocidad, y junto con la aparición de las tecnologías de la información se han modificado todos los procesos de acceso a la información, tanto por parte de los profesionales de los diferentes ámbitos como por los ciudadanos en general. Estamos ante un mercado global de información en el que cualquiera puede ser emisor y receptor.

Durante los últimos años ha crecido la difusión de las redes sociales. Ningún otro de los servicios web ha tenido una expansión tan alta como las redes sociales. MySpace, LinkedIn, Orkut o Facebook han ganado una enorme popularidad durante los pasados años debido principalmente a la creciente demanda de comunicación y colaboración entre los usuarios.

La web ya no es sólo una vía de comunicación en un único sentido sino que corresponde a la idea de una Internet participativa. Hay cientos, de redes sociales, que dan soporte a un amplio conjunto de intereses y prácticas.

Las redes “son formas de interacción social, definida como un intercambio dinámico entre personas, grupos e instituciones en contextos de complejidad. Un sistema abierto y en construcción permanente que involucra a conjuntos que se identifican en las mismas necesidades y problemáticas y que se organizan para potenciar sus recursos”

Pero el uso de las redes sociales comportan ciertos riesgos en cuanto a la vulneración o al menos la puesta en peligro de derechos como la intimidad personal y familiar, el honor y la propia imagen, es la llamada privacidad electrónica (e-privacidad).

Desde que un usuario se da de alta en una red social pública facilita una gran cantidad de datos personales e información sobre sí mismo, desde nombre, apellidos, fecha de nacimiento, pero más aún a través del perfil (identidad digital) puede describir su actividad diaria, relaciones familiares, preferencias, gustos tendencias etc., y todo ello amplificado por la interrelación en la Red.

Este mundo paralelo que constituyen las redes sociales, es motivo de preocupación para organizaciones nacionales e internacionales.

En la Unión Europea (y en España) la e-privacidad o privacidad electrónica ha quedado reducida a la cuestión de la protección de datos personales en bases de datos automatizadas regulado en la Directiva 95/46/CE pero es evidente que el marco jurídico proporcionado por la norma europea, ya no es suficiente para el “movimiento de información” que posibilitan las redes sociales.

La e-privacidad es difícil de proteger desde la normativa existente ya que en esta el derecho a la protección de datos está pensado para posibles infracciones por parte de los poderes públicos en cambio la privacidad de las redes sociales las ponen en peligro preferentemente los particulares que ofrecen este servicio en Internet, además en las redes sociales no todos los riesgos provienen de posibles bases de datos.

En el marco normativo europeo, la preocupación por la regulación de la protección de los datos personales no es nueva. El Convenio 108 del Consejo de Europa, marcó el inicio de una serie de instrumentos regulatorios que tendrían su continuidad en la Directiva 95/46/CE sobre protección en el tratamiento de datos personales y la libre circulación de esos datos o en la más específica 97/66/CE relativa al tratamiento de los datos personales

y protección de la intimidad en el sector de las Telecomunicaciones. Al mismo tiempo, iniciativas procedentes de la comunidad empresarial y los grupos profesionales, han intentado establecer códigos de conducta —*soft law*— como métodos de unificación jurídica complementarios a la alternativa reguladora.

Es fundamental entender la importancia de la protección de los datos personales en este ámbito, se trata de proteger la propia identidad individual en un marco global de comunicación, en el que ya no existen fronteras geográfica y aún menos fronteras de carácter tecnológico.

Los acercamientos multilaterales a la regulación de las transferencias internacionales de datos tienen su origen en el Convenio de Estrasburgo de 28 de enero de 1981, que va a constituir el antecedente más directo de la Directiva 95/46/CE. Ambos textos legislativos van a tener su justificación en la necesidad de uniformar las distintas regulaciones nacionales en una materia que por su especificidad reclamaba criterios normativos homogéneos.

A modo de síntesis la ***Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de la personal físicas en lo que respecta al tratamiento de los datos personales y a la libre circulación de datos***, constituye el texto de referencia, a escala europea, en materia de protección de datos personales.

Esta Directiva crea un marco regulador destinado a establecer un equilibrio entre un nivel elevado de protección de la vida privada de las personas y la libre circulación de datos personales dentro de la Unión Europea (UE). Con ese objeto, la Directiva fija límites estrictos para la recogida y utilización de los datos personales y solicita la creación, en cada Estado miembro, de un organismo nacional independiente encargado de la protección de los mencionados datos.

La Directiva se aplica a los datos tratados por medios automatizados, así como a los datos contenidos en un fichero no automatizado o que vayan a figurar en él.

Queda fuera del ámbito de aplicación de la Directiva el tratamiento de los siguientes datos:

a) el efectuado por una persona física en el ejercicio de actividades exclusivamente particulares o domésticas; *¿quedaría fuera, pues de la aplicación de la Directiva las redes sociales en cuanto es la actividad de un particular, al menos en su origen?*

b) el aplicado al ejercicio de actividades no comprendidas en el ámbito de aplicación del Derecho comunitario, tales como la seguridad pública, la defensa o la seguridad del Estado.

La Directiva tiene como objetivo proteger los derechos y las libertades de las personas en lo que respecta al tratamiento de datos personales, estableciendo principios de orientación para determinar la licitud de dicho tratamiento, veamos estos principios:

1.- **La calidad de los datos:** los datos personales serán tratados de manera leal y lícita, y recogidos con fines determinados, explícitos y legítimos. Además, serán exactos y, cuando sea necesario, actualizados.

2.- **La legitimación del tratamiento:** el tratamiento de datos personales sólo podrá efectuarse si el interesado ha dado su consentimiento (derecho a la privacidad por defecto) de forma inequívoca o si el tratamiento es necesario para:

- 1 - la ejecución de un contrato en el que el interesado sea parte, o
- 2 - el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento, o
- 3 - proteger el interés vital del interesado, o
- 4 - el cumplimiento de una misión de interés público, o
- 5 - la satisfacción del interés legítimo perseguido por el responsable del tratamiento.

3.- Se establecen categorías especiales de tratamiento

Deberá prohibirse el tratamiento de datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o

filosóficas y la pertenencia a sindicatos, así como el tratamiento de los datos relativos a la salud o a la sexualidad. *Sin embargo, las redes sociales se han convertido en el escaparate en el que mostramos, nuestras tendencias políticas, religiosas, sexuales, filosóficas y no sólo las que “colgamos” nosotros mismos si no las que surgen de nuestras interrelaciones en la red.*

4.- **El derecho de acceso del interesado a los datos:** todos los interesados deberán tener el derecho de obtener del responsable del tratamiento:

- a- la confirmación de la existencia o inexistencia del tratamiento de datos que le conciernen y la comunicación de los datos objeto de los tratamientos;
- b- la rectificación, la supresión o el bloqueo de los datos cuyo tratamiento no se ajuste a las disposiciones de la Directiva, en particular a causa del carácter incompleto o inexacto de los datos, así como la notificación a los terceros a quienes se hayan comunicado los datos de dichas modificaciones.

5.- **Se podrá limitar el alcance de los principios relativos a la calidad de los datos,** la información del interesado, el derecho de acceso y la publicidad de los tratamientos con objeto de salvaguardar, entre otras cosas, la seguridad del Estado, la defensa, la seguridad pública, la represión de infracciones penales, un interés económico y financiero importante de un Estado miembro o de la UE o la protección del interesado.

En principio es difícilmente aplicable para el caso de las redes sociales, habría que determinar a quien pertenecen nuestros datos una vez decidimos compartirlos en una red social

6.- **El derecho del interesado a oponerse al tratamiento:** el interesado deberá tener derecho a oponerse, por razones legítimas, a que los datos que le conciernen sean objeto de tratamiento. También deberá tener la posibilidad de oponerse, previa petición y sin gastos, al tratamiento de los datos respecto de los cuales se prevea un tratamiento destinado a la prospección. Por último, deberá ser informado antes de que los datos se

comuniquen a terceros a efectos de prospección y tendrá derecho a oponerse a dicha comunicación.

Esta cuestión es especialmente relevante en cuanto al uso que la empresas hacen de nuestros datos obtenidos de las redes, como posteriormente veremos

7.- **La confidencialidad y la seguridad del tratamiento:** las personas que actúen bajo la autoridad del responsable o del encargado del tratamiento, incluido este último, sólo podrán tratar datos personales a los que tengan acceso, cuando se lo encargue el responsable del tratamiento. Por otra parte, el responsable del tratamiento deberá aplicar las medidas adecuadas para la protección de los datos personales contra la destrucción, accidental o ilícita, la pérdida accidental, la alteración, la difusión o el acceso no autorizados.

Hemos de reiterar la pregunta: ¿Quién es el responsable del tratamiento de datos en las redes?

De la lectura de los principios que marcan la Directiva 95/46/CE se deduce que son de muy difícil aplicación en el caso de la redes sociales ya que estas suponen una pérdida de control sobre nuestra información personal.

A la vista de las últimas noticias y de las declaraciones de la Vicepresidenta de la Comisión Europea y responsable de Justicia, Viviane Reding, antes del verano de este año 2011, se presentará una propuesta legislativa con la que se pretende actualizar la normativa comunitaria en materia de protección de datos. La Comisión Europea parece dispuesta a actualizar la para adaptarla a la nueva realidad planteada en los últimos años por Internet.

Una nueva regulación que garantice la confidencialidad de los datos personales de los usuarios de redes sociales y devuelva a estos el control sobre la información que publican en la RED

La reforma va enfocada a regular el almacenamiento de datos personales que no son de interés público. Y también hacerlos desaparecer de Google, Yahoo, Youtube o de la redes sociales si el interesado lo solicita.

Esta iniciativa, denominada “**Derecho a olvido**” pretende proteger la privacidad de los internautas quienes tendrán mayor seguridad de que sus datos no estarán circulando por Internet sin su consentimiento. Esta Ley debe reconocer el derecho del usuario a hacer desaparecer su rastro digital en la Red, y que este borrado pueda hacerse sin complicaciones técnicas, para ello la Unión Europea, deberá conseguir que sitios como Facebook y otras redes sociales eliminen completamente nuestra información personal cuando nos demos de baja, asimismo también pretende garantizará la llamada “privacidad por defecto” de forma que ninguna red o programa pueda hacer públicos nuestros datos sin consentimiento expreso.

La UE aspira a dotar de transparencia este mundo digital. Quiere que los proveedores de servicios de Internet o los buscadores recojan los mínimos datos de los usuarios. Y que lo hagan de manera tan clara como para saber quien los almacena, cómo, con qué finalidad y por cuánto tiempo. Además, se propone simplificar y mejorar el ejercicio de los derechos de acceso, rectificación y supresión de contenidos relacionados con el usuario.

Como ya hemos venido señalado desde el comienzo de este artículo la convergencia de la informática y las telecomunicaciones y el desarrollo de redes abiertas ha estimulado poderosamente el movimiento internacional de datos personales con el consiguiente riesgo de violación de la intimidad. El flujo transfronterizo de datos de carácter personal y el diseño de una normativa reguladora eficaz constituyen un auténtico desafío para el Derecho Internacional Privado. Y ello por varios motivos, entre otros, por la creciente dimensión económica que está cobrando el libre tránsito de la información.

La confianza es un valor imprescindible para que la Red se convierta en uno de los motores del desarrollo social y económico en la Unión Europea, por ello esta nueva Ley deberá dar más control a los usuarios de la red sobre los sistemas de publicidad dirigida, que recopilan datos de navegación y consumo para mostrar anuncios personalizados.

Sin duda las redes poseen un gran valor económico, así cada vez se crean más programas, y empresas que dedican especialmente a ello, que buscan información personal de los usuarios de la red, las empresas utilizan las redes sociales para posicionar sus marcas, pero esto ya no se hace de un modo impersonal sino adaptadas a la edad, al género, a la ubicación geográfica e intereses personales de los destinatarios, datos que ellos mismos han proporcionado al incorporarse a la red.

Hemos superado el marketing online o digital para llegar al Marketing Social, como estrategia que transforma la relación y comunicación corporativa haciéndola más cercana al usuario, pero otro lado supone la captura de información personal que este involuntariamente ha puesto en la Red. Es interesante tener en cuenta que en la Red lo que hasta ahora era la publicidad tradicional pasa a ser desarrollada por los propios integrantes de la Red que difunde productos y servicios a través de sus blogs personales, la implicación del usuario hace que la comunicación sea muy rápida, menos costosa pero capaz de crear fuertes lazos de fidelidad.

Como vemos es necesario aunar privacidad y confianza, entendida esta como un modo de compartir datos pero que a la vez se garantice nuestro derecho a la privacidad, en este caso electrónica, así serán necesarias estrategias flexibles que permitan al usuario definir su política privada.

Esto no solo va a requerir un gran esfuerzo por parte del legislador europeo, sino un gran desarrollo técnico en cuanto a protección tecnológica de acceso a la identificación y una estrecha colaboración de las propias redes sociales.

Emilia Parejo Gala

Secretaria General del CES de Extremadura

Mérida 2011