

*TRATAMIENTO Y PROTECCIÓN DE LA
INFORMACIÓN EN LAS REDES SOCIALES*




S

GARRIGUES

16 de abril de 2009

Miguel Acosta

- A. CONSIDERACIONES PREVIAS. DATOS DE INTERÉS**
 - B. ANÁLISIS DE LOS ASPECTOS JURÍDICOS MÁS RELEVANTES**
 - C. RIESGOS DETECTADOS POR EL REGULADOR EN LAS REDES SOCIALES**
 - D. PROPUESTAS Y RECOMENDACIONES**
- 



CONSIDERACIONES PREVIAS. ALGUNOS DATOS DE INTERÉS

● Origen y evolución

- **1995**, Randy Conrads crea el sitio Web “classmates.com”; **1997**, SixDegrees; **2002** Friendster, Fotolog; **2003**, MySpace, LinkedIn, Hi5, SecondLife; **2004**, Orkut; **2005**, Yahoo!360º, Bebo; **2006**, Facebook, Twitter, Tuenti; **2007**, Lively.
- Número de usuarios de RRSS: **272 millones** a nivel mundial (un 58% de los usuarios de Internet registrados), **41,7 millones** de usuarios en Europa, en España entre el **40% y el 50%** de los usuarios habituales de Internet.
- En Europa se espera que el número de usuarios se incremente hasta los **107,4 millones en 2012**.
- En diciembre de 2008 Facebook tiene la entrada diaria de más de **120 millones de usuarios**.
- Dentro de los 500 sitios web más visitados del mundo se encuentran al menos 5 RRSS (Facebook, MySpace, Hi5, Orkut)
- **7 de cada 10 usuarios** de RRSS son internautas menores de 35 años. 1 de cada 3 jóvenes en España utiliza RRSS.

● **Usos de las RRSS por usuarios españoles:**

- Compartir o subir fotos: 70,9%
- Enviar mensajes privados: 62,1%
- Comentar las fotos de los amigos: 55,0%
- Actualizar el perfil: 52,1%
- Enviar mensajes públicos: 50,2%
- Cotillear: 46,2%
- Etiquetar amigos en las fotos: 34,8%
- Informarse: 25%
- Descargar aplicaciones: 19%
- Descargar juegos/buscar amigos: 9,5%
- Buscar empleo/recomendar profesionales: 8,5%



● Definición, aspectos fundamentales y tipologías

● Definición

Una RS es una forma de interacción entre miembros y/o espacios sociales, pudiéndose definir del modo siguiente: *“Las redes sociales online son servicios prestados a través de Internet que permiten a los usuarios generar un perfil, desde el que hacer públicos datos e información personal y que proporcionan herramientas que permiten interactuar con otros usuarios y localizarlos en función de las características publicadas en sus perfiles”.*

● Aspectos fundamentales

- El modelo de crecimiento de la RS se basa fundamentalmente en la técnica del “boca a boca” o proceso viral.
- Las RRSS ofrecen aplicaciones y funcionalidades diversas: **Comunicación** (ayudan a la puesta en común de conocimiento); **Comunidad** (ayudan a encontrar e integrar comunidades) y **Cooperación** (ayudan a realizar actividades juntos).
- Uno de los principales objetivos de la RS se alcanza en el momento en que sus miembros utilizan el medio *on line* para convocar actos y acciones que tengan efectos en el mundo *off line*.



- Tipología

- RRSS **generalistas o de ocio**, se caracterizan por facilitar y potenciar las relaciones personales entre los usuarios que la componen. Posibles subcategorías:

- Plataformas de intercambio de **contenidos e información** (Youtube, Dalealplay.com, Google video) que ponen a disposición del usuarios herramientas para el intercambio y la publicación de contenidos digitales (video, fotos, texto, etc.).

No son en sentido estricto RRSS ya que la capacidad de interacción entre los usuarios es muy limitada (comentarios o puntuación). Propiamente son **plataformas colaborativas**

- RRSS **basadas en perfiles** (Facebook, Tuenti, Wamba, Orkut, etc.). Es el servicio más representativo de RS y más ampliamente utilizado en Internet.

- Redes de **microblogging o nanoblogging** (Twitter, Yammer). Basan su servicio en la actualización constante de los perfiles de los usuarios mediante mensajes de texto lo que permite poner a disposición del resto de los usuarios información clara, concisa, sencilla y rápida, sobre las actividades que se están llevando a cabo en ese momento, impresiones, pensamientos, publicaciones.

No son en sentido estricto RRSS ya que la capacidad de interacción entre los usuarios es muy limitada. Propiamente son **plataformas colaborativas**

- RRSS de **contenido profesional**, herramientas de ayuda para establecer contactos profesionales con otros usuarios (Xing o LinkedIn).



ANÁLISIS DE LOS ASPECTOS JURÍDICOS MÁS RELEVANTES

- **Protección del Derecho al honor, a la intimidad y a la propia imagen**
 - Ley Orgánica 1/1982, de 5 de mayo, de **Protección Civil del Derecho al Honor**, a la Intimidad Personal y Familiar y a la Propia Imagen.
 - Ley Orgánica 15/2003, de 25 de noviembre, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del **Código Penal**.
 - Ley Orgánica 1/1996, de 15 de enero de Protección Jurídica del menor.
- **Protección de Datos de Carácter Personal**
 - STC 292/2000. Derecho a la autodeterminación informativa. **La protección de datos como Derecho Fundamental**.
 - Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (**LOPD**).
 - Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD (**RLOPD**).



- Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y Comercio Electrónico (**LSSI**).
- Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones (**LGT**).
- Ley 25/2007, de Conservación de Datos relativos a las Comunicaciones Electrónicas y a las Redes Públicas de Comunicaciones, por lo que se refiere al secreto de las comunicaciones y el derecho fundamental de la protección de datos.
- **Protección del Derecho sobre la propiedad intelectual e industrial de contenidos**
 - Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la **Ley de Propiedad Intelectual**.
 - Ley Orgánica 15/2003, de 25 de noviembre, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del **Código Penal**.

- **IV. Protección de los Consumidores y Usuarios**

- Real Decreto legislativo 1/2007, de 16 de noviembre, por el que se aprueba el Texto Refundido de la **Ley General de Defensa de los Consumidores y Usuarios**.
- Ley 7/1996, de 15 de enero, de **Ordenación del Comercio Minorista**, en lo referente a las ventas a distancia.



RIESGOS DETECTADOS POR EL REGULADOR EN LAS REDES SOCIALES

- **Los riesgos se detectan en tres fases diferentes:**
 - Alta como Usuario
 - Participación en la Red
 - Baja del servicio
- Todas las RRSS disponen de avisos legales, condiciones de uso y políticas de privacidad redactadas en un **lenguaje de difícil comprensión** para el usuario medio, por lo que no se consigue el objetivo de que el usuario comprenda el objeto, la finalidad y el plazo para el que son recabados y tratados sus datos personales.

- Riesgos en el momento de registro de **ALTA** como usuario.
 - Que el tipo de **datos solicitados en el formulario de registro sean excesivos** (aunque no sean obligatorios). Habitualmente se pregunta sobre datos sensibles por ser de gran interés para servir a los fines propios de las RRSS.
 - Que el **grado de publicidad del perfil de usuario sea demasiado elevado**. Todas las RRSS analizadas muestran, activado por defecto, el mayor grado de publicidad, resultando el perfil de acceso completamente público.
 - Que la finalidad de los datos no esté correctamente determinada. **Información generalista**.
 - **Transferencia internacional de datos**. La mayoría de las plataformas se encuentran ubicadas fuera del territorio europeo principalmente EE.UU.
 - **Cesión de derechos de propiedad intelectual** a favor de la RS.

- Riesgos en el momento de **PARTICIPACIÓN** en la red como usuario.
 - La **publicación excesiva de información personal** (propio de terceros). Resolución AEPD PS/117/2008.
 - La instalación y uso de “**cookies**” sin conocimiento del usuario.
 - Uso de Web “**Beacons**”. Imágenes electrónicas que permiten al sitio web conocer quién y qué contenido *on line* ha sido visitado.
 - Que el **perfil de usuario sea indexado automáticamente por los buscadores de Internet**. La mayor parte de las plataformas analizadas lo permiten.

En algunos casos, dicha indexación incluye el nombre del usuario registrado, su fotografía del perfil, el nombre y fotografías del perfil de los amigos o contactos con los que se cuenta en la RS.

- La recepción de **publicidad hipercontextualizada**. La publicidad on line es el modelo de explotación comercial más utilizado actualmente.
- La recepción de comunicaciones comerciales no solicitadas (**spam**).
- La **suplantación de identidad** de los usuarios de la red social.

- Riesgos en el momento de darse de **BAJA** de la plataforma.
 - La imposibilidad de realizar la baja efectiva del servicio.
 - La conservación de datos y el cumplimiento del principio de calidad de los datos.

- Riesgos específicos para los **MENORES DE EDAD**.
 - Captación de datos de menores de edad sin observar lo dispuesto en el **RD 1720/2007**.
 - Ciberacoso.
 - Captación de menores.
 - Comportamientos arriesgados de los menores consistentes en revelar información personal excesiva.

PROPUESTAS Y RECOMENDACIONES DEL REGULADOR DIRIGIDAS A LOS DISTINTOS OPERADORES DE REDES SOCIALES

- Principales preocupaciones
 - Calidad de la información que se facilita a los usuarios
 - Comprobación efectiva de la edad de los menores
 - Lucha contra el *spam*
 - Implantación de herramientas tecnológicas que erradiquen o mitiguen significativamente el fraude *on line*.
- La solución o avance en los temas anteriores no se prevé que venga de la mano de un mayor desarrollo legislativo sino por medio de la **AUTORREGULACIÓN** de los distintos agentes intervinientes.
 - Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online. Edición Febrero 2009. Agencia Española de Protección de Datos e INTECO (Instituto Nacional de Tecnologías de la Comunicación)
 - Safer Social Networking Principles for the EU. 10 Febrero 2009

● Propuestas y recomendaciones dirigidas a la industria

● Propuestas y recomendaciones a las RRSS y plataformas colaborativas

■ Recomendaciones tecnológicas y de seguridad

■ **Transparencia y facilidad de acceso a la información.**

- Utilización de lenguaje en condiciones de uso y políticas de privacidad absolutamente comprensible
- Destacar dentro de las páginas de inicio un apartado específico destinado a informar a los usuarios.
- Creación de “**microsites**” con acceso directo desde la página principal, en los que se exponga información mediante “**preguntas frecuentes**” y **contenidos multimedia** (videos, diapositivas *on line*, etc).
- Mantenimiento de la política de privacidad y condiciones de uso **sin cambios** importantes ni trascendentes para los usuarios. De lo contrario, comunicación previa para aceptación.

- Garantizar a los usuarios el control absoluto del tratamiento de sus datos e información publicada en la red.
 - Ejercicio automático de los derechos ARCO.
 - Informar siempre para qué se utilizan los datos personales y la información publicada en el perfil.
 - Limitar la posibilidad de etiquetado de los usuarios dentro de la red, de tal forma que cualquier persona etiquetada con su nombre reciba automáticamente una solicitud de aceptación o rechazo.
 - Que los sistemas de denuncias implementados permitan que el usuario se de baja, bloquee el acceso por parte de cualquier otro usuario a los contenidos denunciados, siendo éste un procedimiento completamente automático y de aplicación inmediata.
 - Configurar por defecto el máximo grado de privacidad del perfil de usuario, permitiéndole que pueda graduarlo en función de sus preferencias.
 - Garantizar la seguridad tecnológica de la plataforma.
 - Qué los servidores DNS sean completamente seguros y no presenten ningún tipo de vulnerabilidad pública.
 - Emplear herramientas especialmente destinadas a detectar, evitar y bloquear casos de *phishing* o *pharming*.
 - Emplear herramientas anti *spam*.

- Implementar medidas tecnológicas que permitan **conocer la edad de los usuarios** (uso de certificados reconocidos de **firma electrónica o DNI electrónico**).
 - Utilización de herramientas que reduzcan los casos de **suplantación de identidad**.
 - Utilización de sistemas que detecten el nivel de seguridad de las contraseñas elegidas por los usuarios en el momento de registro.
 - Empleo de sistemas que **cifren el contenido** alojado en la plataforma.
 - Empleo de herramientas tecnológicas que impidan que cualquier usuario pueda descargar información publicada en los perfiles del resto de usuarios, con independencia del tipo de contenido de que se trate.
 - Recomendación de que se permita y fomente el **uso de seudónimos o nicks de usuario** que permita la creación de auténticas “identidades digitales”.
- Recomendaciones en materia de formación y concienciación de los usuarios sobre la seguridad.
 - Desarrollo interno de espacios web dedicados a poner a disposición de los usuarios el máximo nivel de protección posible.
 - Facilitar información relativa a las medidas de seguridad puestas a disposición de los usuarios.
 - Realización de programas de formación.
 - Llegar a acuerdos con las autoridades nacionales e internacionales competentes para el fomento de la formación y concienciación de los usuarios respecto a la importancia de la seguridad en Internet.

- **Propuesta de recomendaciones dirigidas a los fabricantes y proveedores de servicios de seguridad informática.**
 - Prevención del fraude *on line*.
 - Investigación y desarrollo en materia de seguridad tecnológica.
 - Que las aplicaciones hayan sido desarrolladas, revisadas y evaluadas conforme a criterios estándares de calidad, seguridad y privacidad que garanticen que su utilización es segura y respetuosa con los derechos de los usuarios.
 - Fomento de la interoperabilidad de los sistemas de seguridad.
 - Colaboración directa con las Fuerzas y Cuerpos de Seguridad del Estado en la investigación de nuevas situaciones de riesgos para los usuarios.
 - Detección de códigos malicioso de programación y elaboración de listados (“**Black Listed**”), en los que sean incluidos todos los nombres de dominio que no superen los criterios de seguridad previamente establecidos.
 - Desarrollo de parches de seguridad y actualizaciones.

- Desarrollo de aplicaciones remotas que permitan el control pleno por parte de los tutores de los contenidos y de las operaciones realizadas por los menores a través de Internet (ya existen estos servicios **vía sms**).
- Desarrollo de aplicaciones que permitan a las plataformas controlar la edad de los usuarios que intentan acceder al servicio.
- Incluir en la descripción técnica de los productos de *software* destinados al tratamientos de datos personales, la descripción técnica del **nivel de seguridad** básico, medio o alto de acuerdo con **el RDLOPD**.
- Utilización de herramientas encaminadas a reducir **el spam**.
- **Propuestas y recomendaciones dirigidas a los prestadores de servicios de acceso a Internet.**
 - Creación de plataformas de comunicación fehaciente y segura con las Fuerzas y Cuerpos de Seguridad del Estado, Ministerio Fiscal y Autoridades Judiciales.

- Apoyo y asistencia plena a las Fuerzas y Cuerpos de Seguridad del Estado cuando realicen reclamaciones a las mismas.
- Informar a todos los usuarios y clientes directos sobre las medidas de seguridad que mantiene respecto al servicio concreto.
- Atender inmediatamente las reclamaciones de bloqueo de servicios cuando se reciban por cualquier método que deje constancia de la identidad del remitente y se identifique de forma clara y concisa el emisor del mismo.

● **Propuestas y recomendaciones dirigidas a las Administraciones e Instituciones Públicas.**

● Desde el punto de vista normativo.

- Necesidad de equiparar los requisitos normativos del mundo digital con los del físico, de tal forma que las condiciones para la prestación de servicios digitales no sean más gravosos que para su prestación en el mundo real.

La gran mayoría de los consultados no ven necesaria una reforma normativa completa, requiriendo únicamente una mejor interpretación de la normativa con la que actualmente se cuenta.

- Promover la elaboración de informes, recomendaciones y dictámenes públicos, en los que se analicen periódicamente los servicios de Internet más utilizados por los ciudadanos españoles.
- Que se fomente el establecimiento internacional, al menos al nivel comunitario, de los principios normativos básicos tendiendo a una seguridad jurídica global.
- Deberá garantizarse la **ejecución efectiva de las sanciones** para aquellas plataformas o usuarios que compartan u obtengan información de forma ilegal.
- Trabajar en favor de un **derecho internacional homogéneo** en materia de protección de datos personales, honor, intimidad y propia imagen, que permitan la correcta protección de los mismos en Internet.

- Desde el punto de vista ejecutivo y administrativo
 - Formación específica en Derecho Tecnológico destinada a jueces, magistrados, forenses, fiscales y secretarios judiciales y cualquier otro cuerpo de la administración pública relacionados con los servicios de la sociedad de la información.
 - Dotar a las brigadas tecnológicas de las Fuerzas y Cuerpos de Seguridad del Estado de herramientas tecnológicas que les permitan investigar, mantener la cadena de custodia de las pruebas electrónicas y bloquear situaciones que pudieran ser susceptibles de delitos y/o perjudiciales para los usuarios.
 - Desarrollo y articulación de procedimientos judiciales rápidos y gratuitos.
- Desde el punto de vista formativo y divulgativo
 - Campañas de concienciación sobre riesgos de la difusión de datos personales en las RRSS.
 - Jornadas de formación y programas de difusión.
 - Incluir en los planes oficiales de estudio el conocimiento de aspectos relacionados con la seguridad de las tecnologías de la información y la protección de datos personales.
 - Acciones de sensibilización y fomento de la seguridad en Internet

- **Propuestas y recomendaciones dirigidas a los usuarios y asociaciones.**
 - Protección de datos personales, honor, intimidad y propia imagen.
 - Disponer de un perfil registrado en el que no se publique información excesiva respecto a su vida personal y familiar.
 - Recurrir al uso de seudónimos o *nicks* personales con los que operar a través de Internet, de tal forma que el usuario únicamente será conocido por su círculo de contactos, que conocen el *nick* que emplea en Internet.
 - Prestar especial cuidado a la hora de publicar contenidos audiovisuales y gráficos en sus perfiles, dado que pueden estar poniendo en riesgo la privacidad e intimidad de personas de su entorno.
 - Revisar y leer las condiciones generales de uso y la política de privacidad que la plataforma pone a su disposición en sus sitios web.
 - Configurar adecuadamente el grado de perfil de usuario en la red social.
 - Aceptar como contacto únicamente aquellas personas conocidas.
 - No publicar en el perfil de usuario información de contacto físico.
 - A los usuarios de herramientas de *microblogging*, no publicar información relativa a los lugares en que se encuentra en todo momento.

- Tecnológicas y de seguridad
 - Emplear diferentes nombres de usuarios y contraseñas para entrar en las distintas redes sociales de las que se sea miembro
 - Utilizar **contraseñas con una extensión mínima de 8 caracteres**, alfanuméricos y con uso de mayúsculas y minúsculas.
 - Disponer en sus equipos de *software* antivirus instalado y debidamente actualizado.
- Protección de menores
 - Recomendaciones dirigidas a menores
 - No se deben revelar datos personales excesivos
 - Lectura de toda la información concerniente a la página web.
 - Si el usuario es menor de 14 años, se necesita el consentimiento de padres y tutores.
 - No deben comunicarse a terceros los nombres de usuarios y contraseñas, ni compartirlos entre amigos o compañeros de clase.
 - Recomendaciones dirigidas a padres y tutores
 - Se debe mantener el ordenador en una zona común de la casa o, en caso contrario, se recomienda utilizar herramientas de monitorización que permitan conocer las rutas de navegación de los menores y que estos no puedan eliminar ni desbloquear dichos contenidos.

- Activar el control parental y las herramientas de control de la plataforma así como establecer el correo del padre o tutor como correo de contacto secundario.
- Asegurarse de que los controles de verificación de la edad están implementados.
- Asegurar la correcta instalación del bloqueador de contenidos.
- Concienciar e informar a los menores sobre aspectos relativos a la seguridad.
- Controlar el perfil de usuario del menor.
- Asegurarse de que el menor solo accede a las páginas recomendadas para su edad.
- Asegurarse de que los menores no utilizan su nombre completo

* * *

Gracias por vuestra atención

Miguel Acosta

miguel.acosta@garrigues.com

GARRIGUES

Avinguda Diagonal, 654 - 08034 Barcelona

Telf.: 93 253 37 00

www.garrigues.com