30 Conferencia Internacional de Autoridades de Protección de Datos y privacidad

Estrasburgo, 15-17 de octubre de 2008

Resolución

sobre

Protección de la privacidad en los servicios de redes sociales

Resolución

En los últimos tiempos, los servicios de redes sociales[1] han experimentado gran auge entre el público. Entre otras cosas, estos servicios ofrecen medios de interacción basados en perfiles personales que generan sus propios usuarios registrados, lo que ha propiciado un nivel sin precedentes de divulgación de información de carácter personal de las personas interesados (y de terceros). Aunque los servicios de redes sociales aportan un amplio abanico de oportunidades de comunicación, así como el intercambio en tiempo real de todo tipo de información, la utilización de estos servicios puede plantear riesgos para la privacidad de sus usuarios (y de terceras personas): los datos personales relativos a las personas son accesibles de forma pública y global, de una manera y en unas cantidades nunca sin precedentes, incluidas enormes cantidades de fotografías y vídeos digitales.

Las personas se enfrentan a posibles pérdidas de control sobre la forma en que terceros emplearán la información una vez publicada en la red: aunque la base "de comunidad" de las redes sociales sugiere que la publicación de los datos personales de carácter privado sería comparable a compartir información con amigos de forma presencial, en realidad la información de cada perfil está disponible para toda una comunidad de usuarios (que pueden ascender a millones).

Actualmente, existe muy poca protección frente a la copia de todo tipo de datos personales en estos perfiles (por parte de los miembros de la red o de terceras personas sin autorización y ajenas a la red), así como frente a su utilización para crear perfiles personales o volver a publicar dichos datos en cualquier otro lugar. Puede resultar muy arduo (y en ocasiones, imposible) eliminar por completo determinada información una vez que ha sido publicada en Internet: incluso una vez que ha sido eliminada del sitio original (p.ej.: la red social), es posible que terce-

[1] "Los servicios de redes sociales se centran en crear y verificar las redes sociales en línea de comunidades de personas que comparten intereses y actividades o que están interesadas en explorar los intereses y actividades de otros […]. La mayoría de estos servicios se ofrecen principalmente a través de Internet y proporcionan un conjunto de métodos de interactuación entre usuarios […]". Traducido de Wikipedia: http://en.wikipedia.org/wiki/Social_network_service.

ras partes o los propios proveedores de los servicios de redes sociales conserven copias. Los datos de carácter personal procedentes de perfiles también pueden "filtrarse" fuera de la red cuando son indexados por motores de búsqueda. Además, algunos proveedores de servicios de redes sociales facilitan datos de los usuarios a terceras partes a través de "interfaces de programación de aplicaciones", que, en ese momento, pasan a ser controlada por dichas terceras partes.

Un ejemplo de usos secundarios que ha captado la atención del público es la práctica de responsables de personal de algunas empresas que investigan los perfiles de candidatos a un puesto de trabajo o incluso de empleados: según algunos informes de prensa, un tercio de los responsables de recursos humanos admite emplear datos de servicios de redes sociales en su trabajo para comprobar y/ o completar detalles de los candidatos a un puesto de trabajo.

Los proveedores de servicios de redes sociales también utilizan la información de los perfiles y de los datos sobre tráfico para emitir mensajes de marketing personalizado a sus usuarios.

Es muy probable que en el futuro surjan otros usos no esperados de la información contenida en los perfiles de usuarios.

Otros riesgos específicos de la seguridad y la privacidad que ya se han identificado incluyen el incremento del fraude de la identidad, alimentado por la amplia disponibilidad de datos de carácter personal en perfiles de usuario, así como la posible piratería de perfiles por parte de terceros no autorizados. La 30 Conferencia Internacional de Autoridades de Protección de Datos y de privacidad recuerda que estos riesgos ya se han analizado en el "Report and Guidance on Privacy in Social Network Services" (Informe y asesoramiento sobre la privacidad en los servicios de redes sociales) ("Memorándum de Roma")[2] de la 43 reunión del Grupo de Trabajo Internacional sobre Protección de Datos en las Telecomunicaciones (3-4 de marzo de 2008), así como en el Documento de posición nº 1 de ENISA "Security Issues and Recommendations for Online Social Networks"[3] (Problemas y recomendaciones de seguridad aplicados a las redes sociales en línea) (octubre de 2007).

Las Autoridades de protección de datos y privacidad reunidos en la Conferencia Internacional están convencidos de la necesidad de realizar, en primera lugar, una amplia campaña de información en la que participen actores públicos y privados (desde organismos gubernamentales a instituciones educativas, desde proveedores de servicios de redes sociales a asociaciones de

[2] http://www.datenschutz-berlin.de/attachments/461/WP_social_network_services.pdf?1208438491
[3] http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_social_networks.pdf

consumidores y usuarios, así como las propias Autoridades de protección de datos y de privacidad) de cara a impedir los muy diversos riesgos asociados con el uso de los servicios de redes sociales.

Recomendaciones

Dado el carácter especial de los servicios, así como los riesgos a corto y a largo plazo para la privacidad de las personas, la Conferencia dalas siguientes recomendaciones a los usuarios de servicios de redes sociales:

Usuarios de servicios de redes sociales

Las organizaciones que estén interesadas en el bienestar de los usuarios de las redes sociales (incluidos los proveedores de servicios, los gobiernos y los organismos para la protección de datos) deberían realizar una labor educativa con los usuarios dirigida a proteger sus datos personales y comunicar los siguientes mensajes.

1. Publicación de información

Los usuarios de servicios de redes sociales deberían plantearse qué datos personales publican –si lo hacen- en un perfil de red social. Deberían ser conscientes de que, posteriormente, podrán ser completados con información o fotografías, por ejemplo a la hora de buscar un empleo. Concretamente, los menores de edad deberían evitar revelar sus domicilios o números de teléfono.

Las personas deberían plantearse la utilidad de usar un seudónimo en lugar de su nombre real cuando creen un perfil. Sea como fuere, deberían ser conscientes de que el uso de un seudónimo ofrece una protección limitada, habida cuenta de que terceras partes podrían apropiarse de dicho seudónimo.

2. Privacidad de otros usuarios

Los usuarios también deberían respetar la privacidad de los demás. Deberán prestar un cuidado especial a la hora de publicar información de carácter personal relativa a otras personas (incluidas las imágenes o fotografías etiquetadas) sin el consentimiento de dichas personas.

Proveedores de servicios de redes sociales

Los proveedores de servicios de redes sociales tienen que considerar una responsabilidad especial y actuar en el interés de las personas que usen las redes sociales. Además de cumplir los requisitos de la legislación en materia de protección de datos, también deberán aplicar las siguientes recomendaciones.

1. Normas y reglamentos sobre privacidad

Los proveedores que operen en diversos países, o que lo hagan a escala global, deberán respetar las normas de privacidad de los países en los que operen sus servicios. Para ello, y si es necesario los proveedores deberán consultar con las autoridades de protección de datos..

2. Información sobre usuarios

Los proveedores de servicios de redes sociales deberán informar, de forma transparente y abierta, a sus usuarios sobre el tratamiento de sus datos de carácter personal. Deberá proporcionarse información fácil e inteligible sobre las posibles consecuencias de publicar datos de carácter personal en un perfil, así como acerca de los riesgos de seguridad y el posible acceso legal por parte de terceros (incluidas las autoridades encargadas de la aplicación de la ley). Dicha información también deberá incluir asesoramiento sobre la manera en que los usuarios deben gestionar la información privada de otras personas incluidas en sus perfiles.

3. Control de usuarios

Los proveedores deberán seguir mejorando el control de los usuarios sobre la utilización que hacen los miembros de la comunidad de los datos contenidos en los perfiles. Deberán permitir una restricción en la visibilidad completa de los perfiles, así como de los datos contenidos en los mismos y en las funciones de búsqueda de las comunidades.

Los proveedores también deberán permitir el control por parte de los usuarios sobre el uso secundario de perfiles y datos de tráfico; por ejemplo en el caso del marketing dirigido a un objetivo. Como mínimo, deberán permitir excluir los datos generales del perfil -opt out- y solicitar el consentimiento expreso para datos sensibles –opt in- (p.ej.: opinión política, orientación sexual) y se deberá aportar datos sobre el tráfico.

4. Configuraciones por defecto que sean respetuosas con la privacidad

Más aún, los proveedores deberán ofrecer configuraciones por defecto que sean respetuosas con la información contenida en los perfiles de usuario. Las configuraciones por defecto desempeñan un papel clave en la protección de la privacidad del usuario: se sabe que solo una minoría de usuarios inscrita en servicios de redes sociales realiza cambios. Dichas configura-

ciones deberán ser específicamente restrictivas cuando un servicio de redes sociales esté dirigido a menores.

5. Seguridad

Los proveedores deberán continuar mejorando y conservando la seguridad de sus sistemas de información y proteger a los usuarios de accesos fraudulentos a sus perfiles, utilizando para ello las mejores prácticas reconocidas en la planificación, desarrollo y ejecución de sus aplicaciones, incluidas auditorías y certificaciones independientes.

6. Derechos de acceso

Los proveedores deberán garantizar a las personas (con independencia de que sean, o no, miembros del servicio de la red social de que se trate), el derecho de acceso y, si procede, de corrección de los datos de carácter personal que obren en poder del Proveedor.

7. Eliminación de perfiles de usuario

Los proveedores también deberán permitir que los usuarios cancelen su pertenencia a una red, eliminen su perfil y todo contenido o información que hayan publicado en la red social de una manera sencilla.

8. Uso del servicio bajo un seudónimo

Los proveedores deberán permitir la creación y utilización de perfiles seudónimos de forma opcional, y fomentar el uso de dicha opción.

9. Acceso de terceros

Los proveedores deberán tomar medidas eficaces para impedir el “spidering” y/ o las descargas en masa (o “bulk harvesting”) de datos de perfil por parte de terceros

10. Indexabilidad de perfiles de usuario

Los proveedores deberán garantizar que los datos de usuarios sólo pueden explorarse en motores de búsqueda externos cuando un usuario haya dado su consentimiento explícito, previo e informado a tal efecto. La no indexabilidad de los perfiles por parte de motores de búsqueda debería ser una opción por defecto.