Nota de prensa

En una resolución aprobada por las autoridades de protección de datos de 37 países en el marco de la 30 Conferencia Internacional de Privacidad

Autoridades de protección de datos advierten de los potenciales peligros para la privacidad de las redes sociales

- **El auge de estos servicios ha propiciado un nivel sin precedentes de divulgación de información personal y fotografías.**
- **Los datos incluidos en los perfiles de las redes sociales pueden filtrarse fuera ellas cuando son indexados por los buscadores.**
- **Se alerta sobre el incremento de fraude de identidad, por la amplia disponibilidad de datos personales en los perfiles de sus usuarios.**
- **Responsables de personal de algunas empresas suelen investigar los perfiles de candidatos a un puesto de trabajo o empleado.**
- **Se recomienda a los menores evitar revelar sus domicilios o números de teléfono.**

(Madrid, 23 de octubre de 2008). Autoridades de protección de datos y privacidad de más de 37 países han adoptado, en el marco de la 30 Conferencia Internacional de Privacidad celebrada en Estrasburgo, una Resolución relativa a la protección de la privacidad en redes sociales.

En dicha Resolución se destaca que el **auge experimentado por estos servicios ha propiciado un nivel sin precedentes de divulgación de información personal y se advierte** de los potenciales riesgos para la privacidad de sus usuarios y de terceras personas al encontrarse **la información de cada perfil,** incluidas gran cantidad de fotografías y videos, **disponible para toda una comunidad de usuarios, que pueden acceder a millones de ellos**.

Asimismo se incide en la existencia de **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 ajenas a ella.** Además se destaca el hecho de que **los datos personales incluidos en los perfiles de las redes sociales pueden filtrarse fuera de esta red cuando son indexados por los buscadores.**

En la resolución **se recogen,** co**mo ejemplo de usos secundarios y de riesgos potenciales** para la privacidad de los usuarios, **la práctica de responsables de personal de algunas empresas que investigan los perfiles de candidatos a un puesto de trabajo o empleado**. También se destaca el hecho de que los propios proveedores de servicios de las redes sociales **utilicen la información de sus usuarios para emitir mensajes de marketing personalizado a sus usuarios**.

En especial **se alerta sobre el incremento de fraude de identidad,** alimentado por la amplia disponibilidad de datos personales en los perfiles de sus usuarios.

En este sentido las Autoridades de Protección de Datos han destacado en la resolución **la necesidad de realizar una amplia campaña de información** en la que participen actores

públicos y privados, de cara a impedir los diversos riesgos asociados con el uso de las redes sociales, y han adoptado, entre otras, las siguientes recomendaciones:

A los usuarios de servicios de redes sociales

1. Los usuarios de servicios de redes sociales deberían plantearse qué datos personales publican en un perfil de red social. Deberían ser conscientes de que, posteriormente, podrán ser completados con información o fotografías, por ejemplo al buscar un empleo.
2. Los menores de edad deberían evitar revelar sus domicilios o números de teléfono.
3. Las personas deberían plantearse la utilidad de usar un seudónimo en lugar de su nombre real cuando creen un perfil.
4. Los usuarios 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.

A los Proveedores de servicios de redes sociales

1. 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 . 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.**
5. Seguridad. Los proveedores deberán continuar mejorando y conservando la seguridad de sus sistemas de información y p**roteger 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.
7. Eliminación de perfiles de usuario. Los proveedores también deb**e**rán 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 las descargas en masa de datos de perfil por parte de terceros.
10. Indexabilidad por buscadores de perfiles de usuario. Los proveedores deberán garantizar que los datos de usuarios **sólo pueden explorarse en buscadores 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.