

Mañana se celebra en Europa el “Día de la protección de datos”

La AEPD elabora un decálogo de recomendaciones, apelando a la responsabilidad de los usuarios de Internet

- Para la AEPD resulta prioritario crear en la ciudadanía una cultura para la protección de sus datos en Internet, principalmente en entornos como redes sociales.
- En 2009 la AEPD recibió las primeras denuncias relacionadas con redes sociales, más de 30, relacionadas con casos de suplantación de identidad o publicación de fotos sin consentimiento.
- La AEPD apela a la responsabilidad de los internautas en las redes sociales ante las posibilidades de difusión de datos o fotografías y videos de terceras personas.

(Madrid, 27 de enero de 2010). Mañana 28 de enero se celebra en Europa [“el Día de Protección de Datos”](#), una jornada promovida por el Consejo de Europa, la Comisión Europea y todas las autoridades de protección de datos de los países miembros de la Unión Europea, con el objetivo de **impulsar el conocimiento entre los ciudadanos europeos** de cuáles son sus derechos y responsabilidades en materia de protección de datos.

En España las últimas encuestas revelan que los ciudadanos tienen muy presente esta materia y que su preocupación por el uso de información personal es creciente. En este sentido, según se desprende del Barómetro de CIS de septiembre de 2009, **el 73,9 por ciento de los ciudadanos se muestra preocupado por la protección de su privacidad**. Asimismo, es destacable el hecho de que **en 2009 el número de reclamaciones planteadas ante la AEPD se haya incrementado en un 75 por ciento, llegando a superar las 4.100**. Para la AEPD estos datos revelan una creciente concienciación de los ciudadanos acerca del valor de su información personal.

En relación a la confianza de los ciudadanos en torno al grado de seguridad de sus datos, según los datos del CIS, un 56,6 por ciento de los ciudadanos españoles destacan que Internet les ofrece una seguridad y **privacidad** de los datos baja o muy baja, y **más del 70 por ciento cree que el uso de Internet favorece la intromisión en la vida privada de las personas**. Estos datos están en conexión, con **la proliferación de denuncias y solicitudes de tutelas de derechos** relacionadas con Internet, y con el hecho de que la institución haya recibido el pasado año las **primeras denuncias relacionadas redes sociales**, más de 30, relacionadas con casos de suplantación de identidad o publicación de fotos sin consentimiento.

Para la AEPD resulta prioritario crear en la ciudadanía una **cultura para la protección de sus datos en Internet, principalmente en entornos como redes sociales, y por este motivo, con motivo de la celebración del Día de la Protección de Datos ha elaborado una serie de recomendaciones y consejos prácticos**.

- ❖ **No grabar ni publicar imágenes, videos sin el consentimiento de las personas**. Debe recordar que cuando publica una foto o escribe en un foro puede estar incluyendo información sobre otras personas. Respete sus derechos y sea consciente de su responsabilidad, personal y jurídica.

- ❖ Las redes sociales son una importante fuente para la obtención de información sobre las personas. Debe garantizar la seguridad de su información **mediante una configuración adecuada de su perfil** y utilizando contraseñas adecuadas, y ser consciente de que los buscadores pueden permitir a cualquier tercero obtener la información pública de los perfiles.
- ❖ **No publicar en los perfiles de las redes sociales excesiva información personal y familiar** (ni datos que permitan la localización física), y **no aceptar solicitudes de contacto de forma compulsiva**, sino únicamente a personas conocidas o con las que haya relación previa.
- ❖ **Precaución, ya que en Internet no todo el mundo es quien dice ser.** Si cuando le solicitan sus datos no le dicen para qué los van a usar, o no entiende lo que le dicen: nunca dé sus datos.
- ❖ Tener especial cuidado al publicar información relativa a los lugares en que el usuario o un tercero se encuentra en todo momento. Podría poner en peligro a los usuarios.
- ❖ **Navegue con los menores:** debe acompañarse a los menores, ayudarles a distinguir los riesgos, asegurarse de que los niños no accedan a Internet a través de entornos no confiables o de que no intercambien datos personales ni fotografías con desconocidos.
- ❖ **Cuando envíe mensajes de correo a una variedad de destinatarios**, utilice el campo "Con Copia Oculta (CCO)".
- ❖ **Comercio y Banca electrónica.** Antes de aportar ningún tipo de datos personales debe asegurarse de que se ha establecido una conexión segura con el portal. Desconfíe de los correos electrónicos que informan de cambios en las políticas de seguridad y solicitan datos personales y claves de acceso.
- ❖ **No es conveniente contestar al Spam.** Es conveniente desactivar la opción que envía un acuse de recibo al remitente de los mensajes leídos del sistema de correo electrónico. Si un spammer recibe dicho acuse sabrá que la dirección está activa, y lo más probable es que le envíe más Spam.
- ❖ **Leer detenidamente las Políticas de Privacidad y las Condiciones de Cancelación.** Si se va a suscribir a un servicio on line o a contratar un producto, revise la política de privacidad. No dude en ejercer los derechos de acceso y cancelación sobre sus datos ante estas empresas.

Asimismo, la AEPD **insta a los responsables de los servicios de Internet** que permiten estas actividades a:

- ❖ Informar sobre los deberes de los usuarios en los procedimientos de alta y registro.
- ❖ Redactar las condiciones de uso y políticas de privacidad con un lenguaje comprensible, para que cualquier tipo de usuario tenga claros sus derechos y obligaciones.
- ❖ Poner a disposición del usuario herramientas que le otorguen el control absoluto de la información que publica en la red; es decir, medios que limiten la posibilidad de etiquetar a otros usuarios (recibiendo automáticamente una solicitud de aceptación o rechazo).
- ❖ Establecer cambios en la configuración del nivel de privacidad, de forma que se establezca, por defecto, el máximo grado de seguridad en el perfil del usuario (generalmente permite la máxima difusión de los perfiles).
- ❖ Implantar sistemas que faciliten la comprobación de la edad de los usuarios que intenten acceder al servicio, reduzcan los casos de suplantación de identidad (bloqueando el acceso al usuario que utilizó el perfil de otro de forma ilegítima) o detecten el nivel de seguridad de las contraseñas elegidas (e informen de los mínimos aconsejables) .

- ❖ Rectificar o retirar la información cuando lo solicite un afectado de modo justificado.
- ❖ Controlar de la indexación y almacenamiento de los perfiles por parte de los buscadores.
- ❖ Elaborar y publicar códigos éticos que garanticen unas mínimas reglas de actuación de los usuarios o de las comunidades en las redes sociales.