



## "La gente tiende a dejar rastros en internet sin ningún cuidado"

**Ciber-crimen, pérdida de privacidad, niños que usan internet... el progreso técnico hace necesario adaptar las normas sobre protección de datos constantemente. La UE trabaja en estos momentos en una revisión de la directiva comunitaria sobre el tema; el ponente en la Eurocámara, el europarlamentario popular alemán Axel Voss, explica que "los consumidores deben poder controlar sus datos en internet, saber cuáles comparten, dónde se almacenan y para qué se van a usar".**

Su proyecto de informe sobre un enfoque global de la protección de los datos personales en la Unión Europea fue apoyado la semana pasada por la comisión de Libertades Civiles del Parlamento Europeo. Representa la respuesta de la Eurocámara a la comunicación sobre el tema que fue hecha pública por la Comisión Europea en noviembre.

**Señor Voss, ¿cuáles son los principales retos para la protección de los datos y la privacidad en la UE?**

En primer lugar está el constante progreso técnico y las nuevas aplicaciones que crea. La web 2.0, las redes sociales, los servicios de geolocalización o los teléfonos inteligentes no podían ni imaginarse cuando se adoptó la actual legislación sobre protección de datos. Hay que modernizarla para incluir los desarrollos técnicos y garantizar la protección de los datos de los ciudadanos europeos en el futuro.

En segundo lugar, la directiva europea de 1995 es una base bastante buena, pero se está aplicando con dificultades en los Estados miembros. Las empresas tienen que ajustarse a un abanico de distintas leyes sobre privacidad; necesitamos una norma uniforme para toda la UE.

Es más, la aplicación es la clave: la regulación europea sobre protección de datos tiene que estar en vigor en cualquier lugar en el que se procesen datos de un ciudadano europeo. Este punto es clave, si pensamos que hay servicios que se dirigen a ciudadanos europeos desde Estados Unidos o Asia.

**¿Y qué me dice de la criminalidad en internet? ¿También supone un desafío para la protección de datos?**

Cada vez hay más ciber-crimen, y es muy difícil perseguir a los criminales y llevarlos a juicio. En este sentido, también creo que los ciudadanos tienen una responsabilidad sobre sus propios datos. Tenemos que ayudar a la gente a ser consciente de lo que hacen en internet, ayudar a los consumidores a conocer los riesgos para que sean menos descuidados con sus datos. La mejor protección es siempre la que hace uno mismo. Hoy en día, la gente tiende a dejar rastros en internet sin ningún cuidado.

}

Pero no sólo hay que responsabilizar al consumidor. Soy muy partidario de la introducción de un principio sobre la obligación de rendir cuentas de los controladores de datos, es decir, las empresas. Es más, mis colegas y yo votamos a favor de la aplicación general de notificaciones de violaciones de datos, que ya conocemos por el sector de las telecomunicaciones. Si, por ejemplo, se está robando de servidores de empresas la información sobre tarjetas de crédito de unos millones de personas, los responsables de esas empresas

tienen que informar inmediatamente a los afectados para que puedan tomar las medidas necesarias para proteger su privacidad y ser compensados por las pérdidas. Escándalos recientes demuestran que este no es el caso ahora mismo.

## **En su informe habla de principios nuevos como la «privacidad por diseño» y « por defecto». ¿Qué significan?**

Estos principios tienen como objetivo reducir la cantidad de datos que los ingenios técnicos comparten de forma automática. Pedimos a los fabricantes y desarrolladores que integren desde el primer momento mecanismos que minimicen el almacenamiento de datos, Es decir, que haya "privacidad por diseño".

La privacidad por defecto significa que cuando haga uso de un producto el consumidor debe encontrarlo preconfigurado con los máximos estándares de privacidad. Hoy, muchas veces tenemos que cambiar las preferencias si queremos más privacidad, y a veces es complicadísimo. Queremos darle la vuelta al planteamiento: si quieres revelar más información sobre ti, tendrás que cambiar a propósito las preferencias. La gente debe tener derecho a decidir cuánto quieren que sea visible, y esa decisión no debe impedir que accedan a determinados servicios.

### **Principios sobre protección de datos**

- La recopilación y almacenamiento de datos requieren consentimiento previo del usuario
- La recogida de datos debe hacerse de forma transparente
- Los consumidores y las empresas deben minimizar la cantidad de datos disponible
- Los datos deben recogerse con un objetivo concreto