

‘Los gobiernos sufren ataques de hackers’

POR JAVIER DÍAZ PLAZA

¿Las nuevas tecnologías de la información y la comunicación son seguras?

Los sistemas son muy seguros, podemos introducir el número de la VISA sin que pase nada. El problema es cómo preservar la privacidad del individuo. Las grandes empresas saben cómo asegurarse, pero el individuo a veces interactúa con la sociedad de la información sin emplear los métodos adecuados para protegerse.

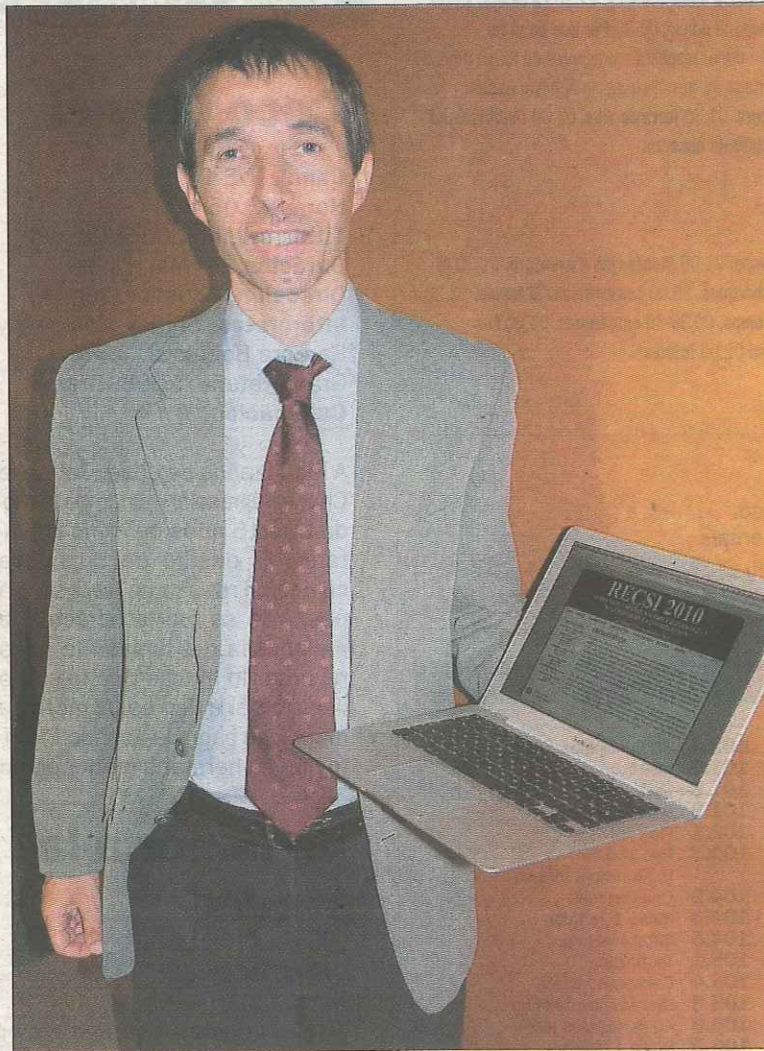
¿Cuáles son las amenazas?

Por un lado, los Estados, que nos venden la historia de que para dar seguridad a los ciudadanos hay que reducirles su privacidad. Ponen cámaras de vigilancia, miran nuestro cuerpo en los aeropuertos, nos toman los datos biométricos... Una serie de cosas que dudo que sean necesarias. Seguramente hay otras medidas que darían el mismo nivel de seguridad sin entrar en la vida diaria de las personas. Al ciudadano honrado se le ha de molestar lo menos posible. El otro factor que contamina es la funcionalidad a expensas de la privacidad.

¿A qué se refiere?

Por ejemplo, Google ofrece gratis el almacenamiento de

PERFIL | Josep Domingo (Sabadell, 1965) es catedrático de Ciencia de la Computación e investigador ICREA Acadèmia en la URV, donde dirige la Cátedra UNESCO de Privacidad de Datos y el departamento de Ingeniería Informática y Matemáticas.



► Josep Domingo presidió el comité organizador de la Reunión Española de Criptología y Seguridad de la Información celebrada en TGN. FOTO: J. DÍAZ

tus datos en internet o una cuenta de correo infinita. Es muy atractivo, pero implica que tus datos están en manos de alguien que no conoces. No quiero decir que haya alguna persona mirando lo que escribes, pero sí que hay una máquina que hace una prospección automática de tus mensajes para ver lo que te interesa. Si le envías un correo a un amigo diciéndole que te vas a las Bahamas, al cabo de pocos días verás en tu cuenta un anuncio sobre las Bahamas.

¿Cómo se puede combatir esto?

No se puede. Para utilizar sus servicios alcanzas un trato con ellos. En las condiciones que hay que aceptar al principio, y que nadie se lee, te dicen que pueden examinar tus datos. Estas empresas utilizan normalmente la formación de manera interna, para enviar propaganda. Pero si, algún día, la policía o el FBI les exigieran tus datos, se los darían.

Los expertos en seguridad informática hablan de espías, intrusos... Parece una película de James Bond.

Aquellos que trabajan con Windows están expuestos a que les coloquen algún virus para capturar su contraseña bancaria. Pero, aparte de eso,

las personas particulares no suponen un gran interés para los espías. Evidentemente, para ellos son mucho más atractivas las instalaciones centrales de un banco, de un gobierno o militares.

¿Los gobiernos son atacados por hackers como vemos en el cine?

Si el sistema operativo no está bien diseñado, sí es posible. Pero cuando a un gobierno le pasa algo así trata de esconderlo. En la India, por ejemplo, están muy preocupados por la ciberseguridad porque tienen muchos enemigos políticos que constantemente les están atacando.

¿Internet es un paraíso para estafadores y delincuentes? Internet es como la calle, puede circular por ella todo el mundo. Si dejas abierta la puerta de tu casa puede entrar cualquiera, y en la Red sucede lo mismo.

Mucha gente es reacia aún a dar sus datos bancarios o hacer compras por internet. Si no tienes virus no pasa nada. En general, es más inseguro darle la tarjeta de crédito a un camarero en un bar, que se la lleva dentro y no sabes lo que está haciendo, que pagar por internet.