EN NOMBRE PROPIO

Pedro Rodríguez López de Lemus *Abogado especializado*

«Un usuario normal de internet está expuesto a que cualquiera le espíe»

Este abogado advierte de los riesgos que corren muchas personas por renunciar a parcelas de su intimidad para beneficiarse de las bondades de las nuevas tecnologías

¿Tienen las nuevas tecnologías un lado oscuro?
—Por supuesto. Tiene muchas bondades pero el mal uso de ellas permite un lado tan oscuro como «el internet profundo» o «deep web», que prácticamente está al margen de la ley y que se puede usar para algo bueno o malo. Cualquier persona puede entrar en ese internet descargándose un programa y navegar anonimamente a través del internet usando una IP aleatoria de un tercero. Ahora mismo esa «deep web» es la pesadilla de los cuerpos y fuerzas de seguridad del Estado.

—¿Están esas fuerzas preparadas para luchar contra el ciberdelito?
—Cada vez más. A partir del 6 de diciembre, que entra en vigor la reforma de Ley de Enjuiciamiento Criminal, los policías podrán con autorización judicial convertirse en agentes encubiertos para perseguir delitos graves como terrorismo, pederastia u organización criminal, y pueden mandar archivos ilícitos o introducir un virus informático para investigar todo lo que hay en nuestro ordenador.

—Si la Agencia Nacional de Seguridad de Estados Unidos espió a más de 30 líderes mundiales, mejor no pensar a qué estamos expuestos seres anónimos como nosotros.
—A todo. A no ser que uses determinadas herramientas, un usuario normal de internet está expuesto a que cualquiera le espíe con o sin derecho a ello. El problema es que las nuevas tecnologías tienen unas bondades a las que no queremos renunciar pero para obtenerlas estamos cediendo parcelas de nuestra privacidad e intimidad sin ser conscientes de ello.

—¿Es necesario ser una hacker experimentada como Lisbeth Salander, la protagonista de Los hombres que no amaban a las mujeres, para acceder a los ordenadores de terceras personas?
—En absoluto. Basta con poner en internet: cómo entrar en una red wifi wap, te descargas un programa en internet, eliges la red y en dos o tres horas tienes la contraseña de una persona que use una red wifi de las antiguas, que hay muchísimas. Cuando estés dentro de la red, hay otro programa que te dice cuáles son las contraseñas del correo electrónico. Hay personas a las que le asignaron wifi sin contraseña y aún no lo saben, con lo que están absolutamente expuestas porque es como si tuvieran la puerta de su casa abierta. Tampoco hace falta meterte en la red wifi de un tercero. Ojo si te vas a una estación de autobuses, de Renfe o Metro y te metes en el wifi público sin usar un certificado electrónico para ocultar tus contraseñas, porque quedas expuesto totalmente.... y una vez que entran en tu correo electrónico estás muerto porque de ahí acceden a tus redes sociales, al banco... a absolutamente casi todo.

—Twitter, Facebook, los comercios, los bancos... acumulan datos nuestros. ¿El Gran Hermano de Orwell está aquí?
—Sí, aunque no queramos verlo. Y esto va a más con los drones que nos vigilan, la Google Glass, los nuevos y pequeñísimos aparatos de videovigilancia... La aplicación Pericospe, que acaba de comprarla Twitter, te permite incluso radiar todo lo que estás haciendo con tu móvil.

—¿No se produce una colisión de intereses cuando hay personas dispuestas a radiar su vida pero al hacerlo informan sobre otras personas que quieren anonimato?
—Hay gente que quieren extimidad, es decir, publicarlo todo. Y la verdad es que quien usa Google Glass no sólo se está grabando a sí mismo, sino también a todo con el que se cruce sin que se lo haya permitido. Se supone que la normativa nos protege pero si hay una moda social y todo el mundo lo hace... Basta pasearse por calles comerciales de Sevilla para darse cuenta de que muchos establecimientos tienen cámaras de videovigilancia apuntando a la calle, algo terminantemente prohibido y sancionado con al menos 40.000 euros por la Agencia de Protección de Datos. Pues adviertes a esas tiendas de que no pueden hacer eso pero como nadie les denuncia... En otras ciudades los policías nacionales y locales denuncian a la Agencia de Protección de Datos cuando las tiendas o particulares tienen cámaras de videovigilancia apuntando a la vía pública. Cualquier persona puede presentar una denuncia ante esa agencia por internet sin abogado ni procurador.

—Las últimas modificaciones legislativas penalizan con la cárcel ciertos comportamientos en la red que antes no eran delito.
—Efectivamente. Antes si tu pareja te había enviado la foto y la divulgabas era difícilmente encajable en el delito de violación del secreto de las comunicaciones. Ese fue el caso de Olvido Hormigos. Ahora sí es delito divulgar imágenes de tu pareja sin su consentimiento.

—¿El acceder a correos electrónicos de otras personas es ya un delito penado con prisión?
—Sí y no sólo eso, sino que es delito tener programas para romper códigos.

—La ciberdelincuencia crece a ritmos de dos dígitos anualmente. ¿Ha cambiado el perfil del delincuente?
—El problema es que no somos conscientes de que estamos cometiendo un delito cuando estamos tranquilamente frente a un ordenador en casa o el despacho. Hay que comportarse igual de bien delante del ordenador que en la calle. Hay gente que no insulta a nadie por la calle pero después lo hace en internet de forma anónima.

—¿Es fácil detectarlos?
—Sí. Te pueden pillar perfectamente porque navegamos con una matrícula en internet, que es la IP. El que sabe de qué va la cosa ya utiliza la «deep web» para que no lo cojan, pero afortunadamente no es lo normal.

—¿Cómo luchar contra los ordenadores zombis dedicados a la ciberdelincuencia?

Acceder a un ordenador
«No hace falta ser un hacker experimentado para acceder a los equipos informáticos de terceras personas»

Wifis públicos
«Ojo con usar wifi público sin ocultar nuestras contraseñas. Si entran en tu correo electrónico estás muerto»

Videovigilancia
«Basta pasearse por Sevilla para ver que muchas tiendas tienen cámaras apuntando a la calle, algo prohibido»