OBSERVATORIO DE LA SEGURIDAD DIGITAL

Las empresas reclaman una mayor seguridad jurídica en Internet

A DEBATE/ Los expertos proponen un pacto para la autorregulación del sector online, combinado con leyes internacionales que protejan los derechos fundamentales de las personas en la Red.

E. Arrieta. Madrid

Más de 430 millones de personas fueron víctimas del cibercrimen el año pasado, sufriendo pérdidas económicas directas de 388.000 millones de dólares (286.539 millones de euros). En España, se contabilizaron 21.936 ataques diarios, con un coste de 482 millones de euros, según un reciente informe de Symantec. "Todas las empresas están expuestas a riesgos. Además, todos sus activos críticos están conectados a una red", expone Guillermo Llorente Ballesteros, subdirector general de Seguridad y Medio Ambiente de Mapfre, durante el Observatorio de la Seguridad Digital organizado por Unidad Editorial, con la colaboración de S2 Grupo.

La complejidad técnica y el desconocimiento de los usuarios incrementan los riesgos. "El ciberespacio no es sólo Internet, es cualquier entorno digital. De hecho, los ataques más dañinos no buscan las redes conectadas a Internet", precisa Óscar Pastor, gerente de Seguridad de Isdefe.

"Usamos los mismos dispositivos para todos los aspectos de nuestras vidas. Al final, el factor humano juega un papel cada vez más relevante en las pérdidas de información de las empresas", recuerda Miguel Ángel Juan Bello, socio director de S2 Grupo.

Aldo Olcese
Miembro de la Real Academia de Economía
"En ocasiones, subimos información a la Red de un modo irresponsable, sin pensar en el uso que otros harán de ella".

Miguel A. Juan Bello
Socio-director de S2 Grupo
"El factor humano juega un peso cada vez más importante. La mayoría de incidentes en la Red está causada por las personas".

Joaquín Álvarez Pérez
Director de Seguridad de la Información de Endesa
"La evolución de la tecnología ha sido tan vertiginosa que nos ha colapsado. Cualquiera con una firma digital puede llegar a firmar lo que sea".

José García Moreno
Director de Recursos Humanos de REE
"En la nube, no está claro qué protección jurídica existe. No es fácil saber dónde se encuentra tu información ni quién puede manejarla".

Joaquín Reyes Vallejo
Dtor. Sistemas de Información de Cepsa
"Ya no se trata de controlar los accesos y procedimientos, sino de integrar la actividad en la Red en la gestión de riesgos de la compañía".

Alejandro Villar Assenza
Subdtor. de Seguridad de la Información de Repsol
"La nube es algo muy positivo. Da la posibilidad a muchas empresas de hacer cosas que, de otro modo, les sería imposible".

Guillermo Llorente
Subdtor. general de Seguridad de Mapfre
"La seguridad es un elemento más en los procesos de la empresa y, por ello, debe ocupar una parte de todos los proyectos".

Fco. Javier García Carmona
Director de Seguridad de Iberdrola
"En la actualidad, existen vacíos legales que dan lugar a un marco de valoraciones diversas ante unas mismas situaciones".

José M. Rosell Tejada
Socio-director de S2 Grupo
"Estos cambios están siendo demasiado rápidos. Por eso, muchas personas no conocen las implicaciones de lo que hacen en la Red".

Manuel Broseta
Socio de Broseta Abogados
"Las leyes españolas no se plasman en una verdadera seguridad en la Red. La norma no es preventiva, sino únicamente la cultura".

Óscar Pastor
Gerente de Seguridad de Isdefe
"Es necesario una regulación internacional, al menos, sobre los derechos fundamentales de las personas en Internet".

Formación

En este contexto, ¿cómo proceder? "Los que no somos *nativos digitales* no sabemos lo peligroso que puede ser, por ejemplo, no tener una contraseña segura. Por eso, son fundamentales la formación y la concienciación como punto de inicio para la concepción de una nueva cultura digital", propone José María Rosell, socio director de S2 Grupo.

"La tecnología existe, pero sobre ésta hacen falta procesos y personas, y que esta cultura digital se extienda por toda la organización desde la alta dirección", coincide Francisco Javier García Carmona, director de Seguridad de Iberdrola. También se muestra partidario de la formación Joaquín Reyes Vallejo, director de Sistemas de Información de Cepsa: "Los trabajadores tienen que saber qué pueden y qué no pueden hacer. La comunicación es válida no sólo para informarles, sino para generar un sentimiento positivo de pertenencia a la empresa. Nadie quiere trabajar en una firma conocida por usurpar delitos personales", asegura.

Reyes Vallejo propone el concepto del riesgo aceptable. "Un ataque online puede afectar a las ventas y a la imagen, pero su prevención requiere también de muchos recursos. Es algo positivo que el control de riesgos hable en el lenguaje de las empresas", opina.

Con todo, la mayor dificultad a la hora de evitar y sancionar muchos de los ataques informáticos estriba en su procedencia internacional. "La mayoría de proveedores de *cloud computing* son multinacionales, lo que dificulta el control de la información. Debería existir un consenso global en este ámbito", dice Alejandro Villar Assenza Parisi, subdirector de Seguridad de la Información de Repsol.

Por eso, muchos ejecutivos en España abogan por la regulación, exclusivamente, de los derechos fundamentales de las personas. "Es necesario una regulación internacional para los derechos fundamentales de las personas en Internet. No es imposible. Tampoco el mar y las guerras tienen fronteras y están sometidas a unas leyes", defiende Pastor.

Regulación internacional

"Hay sentencias suficientes del Tribunal Supremo que aprueban que una empresa imponga sus propias reglas, siempre y cuando éstas integren mecanismos de control y medidas sancionadoras equilibradas", asegura Manuel Broseta, socio de Broseta Abogados.

"Es imposible y, además, carísimo que una empresa asegure al 100% la protección de sus datos. En España, hay una legislación muy amplia y, quizás, excesivamente dura. En Alemania, en cambio, una infracción de este estilo no se penaliza por la vía legal", argumenta este experto.

GUERRA Y MAR

Hasta ámbitos complejos y delicados como las guerras y el transporte de mercancías están sometidos a leyes internacionales. Los empresarios reclaman lo mismo para Internet, en pleno auge de modalidades como el **'cloud computing'**.

La informática en la nube y el miedo a lo desconocido

Por el propio concepto de acceso en remoto, el *cloud computing* (o informática en la nube) se ha identificado siempre como un entorno de riesgo. Bajo esta modalidad, no siempre es fácil situar geográficamente dónde se encuentra cierta información. Tampoco resulta sencillo gestionar los privilegios de accesos a los datos, las auditorías o supervisar el cumplimiento de los protocolos de seguridad del proveedor contratado. "La Unión Europea dictó una directiva que la legislación española ha trasladado a un real decreto, la Ley de Protección de Infraestructuras Críticas. Pero, en la nube, no está claro qué protección jurídica existe", critica José García Moreno, director de Recursos Humanos de REE. Esta compañía optó por organizar una jornada con las familias de los empleados, y en ella se impartieron nociones sobre la seguridad informática. "La nube es algo muy positivo. Da la posibilidad a muchas empresas de hacer cosas que, de otro modo, les sería imposible. El problema es que nadie sabe, a ciencia cierta, qué hay detrás", agrega Villar Assenza Parisi, de Repsol.

"La Agencia Española de Protección de Datos ejerce una defensa sólida sobre los derechos de autor en España, pero hay más por hacer", agrega Joaquín Álvarez, director de Seguridad de la Información de Endesa.

"Internet es la revolución industrial más importante de la historia, pero ninguna revolución puede tener éxito sin eficiencia económica y seguridad jurídica", comenta Aldo Olcese, miembro de la Real Academia de Economía.

Piratería

Olcese, como presidente de la Coalición de Creadores, ha sido testigo de la concepción de normas como la polémica *Ley Sinde*. "Corremos el severo riesgo de que los políticos se vean obligados a regular –posiblemente, mal– ante la falta de consenso en el sector y el clamor de los ciudadanos", afirma.

"Con la piratería, que es el primer ámbito que se ha regulado, las leyes en cada país son diferentes. Si todo sigue igual, en el futuro existirán una veintena de normas dispares para cada cuestión, como la neutralidad de la red y la privacidad, entre otros ámbitos", concluye Olcese.