¿Regular? El gran reto ante internet

Internet lo cambió todo: los aparatos de uso cotidiano están más conectados entre sí, las compañías tienen sus datos más sensibles en línea, la privacidad se volvió un término cada vez más relativo y los riesgos ligados a las nuevas tecnologías se multiplicaron.

Entre estos riesgos destacan el uso indebido de las bases de datos personales y los diferentes tipos de ciberdelincuencia. Enfrentar dichos problemas implica desarrollar herramientas legales que regulen el uso que se le da a Internet y crear una cultura digital más robusta.

¿Qué tanto se ha avanzado en estos temas y dónde está la clave para enfrentar dichos retos?

Datos en todo lugar

Los datos, tanto personales como empresariales, se convirtieron en "oro", según Juan Ignacio Zamora, abogado especialista en tecnologías de la información; y es por eso que protegerlos representa uno de los retos más importantes en la actualidad.

Según Roberto Lemaitre, abogado, ingeniero informático y especialista en delitos informáticos y protección de datos, en el caso de los datos personales los desafíos están relacionados con la explotación comercial indebida de las bases de datos que manejan las compañías de Internet y la confidencialidad.

Esas dos aristas se vuelven aún más sensibles por el desarrollo vertiginoso de "Internet de las cosas", que promueve la incorporación de las tecnologías de Internet en dispositivos de uso diario, como la ropa o los electrodomésticos.


CRM
HRP
010
0010
BUSINESS SOLUTIONS
BUSINESS SUCCESS

Con la red, las bases de datos de diferentes empresas comenzarán a manejar información cada vez más sensible. Por ejemplo, datos sobre la salud de las personas (como los signos vitales), saber si alguien está o no en su casa, o las rutas que se toman a diario con el automóvil.

"El tema de la protección de datos va a ser cada vez más sensible, al ser Internet una tecnología que no tiene marcha atrás. Las empresas van a tener un perfil más exacto de las personas y será peligroso que esa información caiga en las manos equivocadas. Con estos avances, la privacidad se vuelve más relativa y las opciones para la ciberdelincuencia se multiplican", explica Roberto Lemaitre.

Información valiosa

Según datos de la consultora Gartner, en 2020 habrá unos 30 000 millones de dispositivos que van a funcionar con la tecnología de "Internet de las cosas".

Empero, las disputas legales por el manejo de datos ya se están produciendo, principalmente en Europa, la región del mundo que cuenta con una legislación más proteccionista sobre el tema.

La última divergencia importante en el viejo continente fue la relacionada con el "derecho al olvido" y el gigante de las búsquedas Google. El Tribunal de Justicia de la Unión Europea obligó al buscador a borrar, bloquear o suprimir información personal que sea obsoleta por el paso del tiempo o porque afecte algún derecho fundamental, si así lo desea el titular de los datos.

El avance legal referente a la protección de datos es más limitado en Latinoamérica. Sin embargo, según un estudio de la Universidad de Los Andes, el 70% de los países de la región cuenta con disposiciones explícitas referentes a aspectos relacionados con protección de datos personales en Internet.

Costa Rica, por ejemplo, tiene la Ley de Protección de Datos de 2011, texto legal que recoge normas referentes al legítimo tratamiento de los

EL CRIMEN SE MUEVE EN LA RED

Al lado de la protección de datos se encuentra otro de los retos más importantes relacionados con Internet: la ciberdelincuencia.

La ciberdelincuencia, que es cualquier tipo de actividad ilícita donde se utilice Internet, se ha reinventado con el paso del tiempo y representa, en la actualidad, un peligro latente para personas, empresas y gobiernos.

En el caso de las personas, la creación de virus informáticos y plataformas empleadas para robar datos, sigue multiplicándose. Según estimaciones de la empresa de seguridad informática Kaspersky, cada segundo se crean tres nuevos virus informáticos y el 41,6% de los usuarios ha sido víctima de códigos maliciosos. Además, el 15% de los usuarios de redes sociales habría sufrido problemas relacionados con el cibercrimen en sus perfiles.

Las empresas, por su parte, son víctimas de ataques planificados como el que vivió Sony en 2011, cuando un grupo de hackers robó los datos de unos 77 millones de clientes, incluyendo información sensible como números de tarjetas de crédito.

Los gobiernos también sufren el embate de la ciberdelincuencia. Instituciones como el Pentágono, en los Estados Unidos, son atacadas constantemente por ciberdelincuentes. Las amenazas son tan reales que, por ejemplo, el gobierno norteamericano desembolsa unos tres mil millones de dólares al año para protección cibernética.

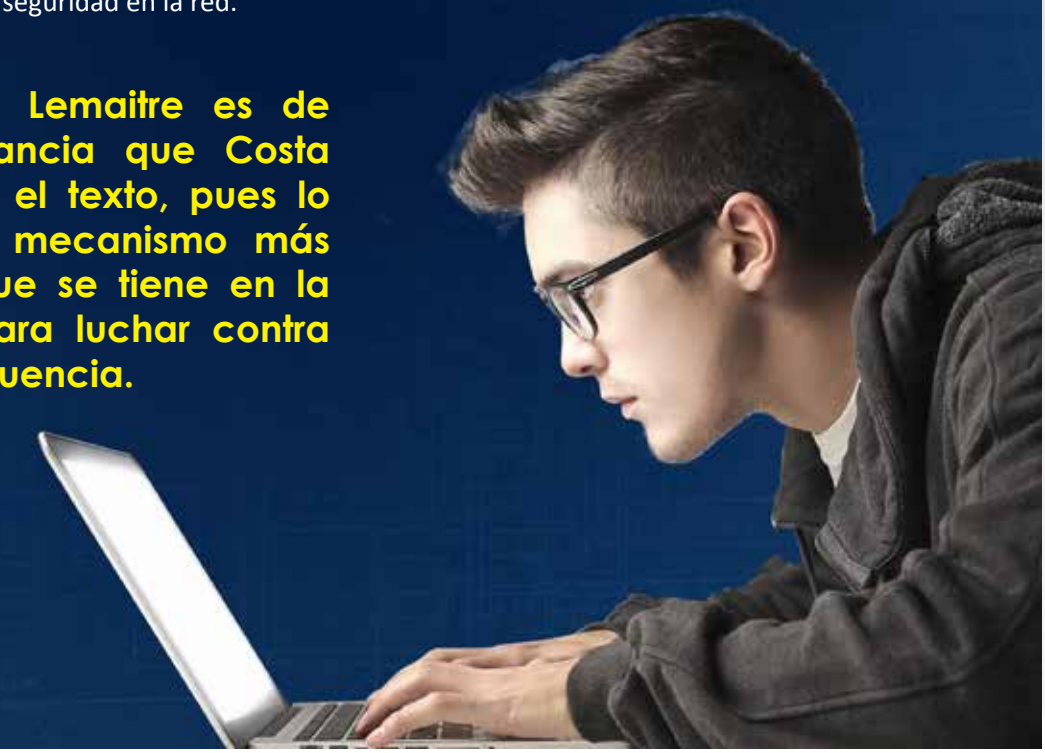
En términos legales, el mayor esfuerzo internacional para hacerle frente a la ciberdelincuencia es la Convención de Budapest o Convenio sobre Cibercriminalidad. Esta convención, que Costa Rica firmó pero no ha ratificado (se encuentra en la corriente legislativa), es el primer tratado internacional sobre delitos cometidos a través de Internet y otras redes informáticas, y aborda infracciones relacionadas con derechos de autor, fraude informático, pornografía infantil, delitos de odio y violaciones de seguridad en la red.

Para Roberto Lemaitre es de suma importancia que Costa Rica ratifique el texto, pues lo considera el mecanismo más importante que se tiene en la actualidad para luchar contra la ciberdelincuencia.

En este campo, el mayor esfuerzo realizado por el país fue una reforma al Código Penal para incluir los delitos informáticos. Entre otras cosas, se sanciona la violación de las comunicaciones, las estafas informáticas, el espionaje y la suplantación de identidad.

Además, el Organismo de Investigación Judicial (OIJ) cuenta con su propia sección de delitos informáticos, instancia responsable de realizar las investigaciones referentes a ciberdelincuencia.

Según la firma Norton, el costo asociado al cibercrimen ascendió a $95 000 millones en 2015 y unos 556 millones de adultos en el mundo fueron en alguna medida víctimas del cibercrimen.



datos personales, al consentimiento previo para el uso de datos y a la rectificación o supresión de estos. Además, prohíbe la transferencia de datos a terceros sin previa autorización.

La ley también creó la Agencia de Protección de Datos de los Habitantes, instancia que vela por el cumplimiento de la protección de datos y resuelve reclamos por infracción a las normas sobre protección.

Juan Ignacio Zamora considera que esta legislación representa un avance importante para el país, pero debe mantenerse actualizada para que sea realmente útil.

¿Y en lo laboral?

Estos dos retos (protección de datos y cibercrimen) son en gran medida más complejos para las empresas, ya que el funcionamiento de las compañías depende cada vez más de las tecnologías de Internet, las cuales están expuestas tanto a ataques directos como indirectos.

Ante esta realidad, Juan Ignacio Zamora considera fundamental que las empresas desarrollen reglamentos internos para regular el uso que se le da a Internet.

"Regular Internet es tratar de regular un monstruo de mil cabezas; es muy difícil, entre otras cosas, porque existen grandes problemas que abordar, como la jurisdicción bajo la cual se debe enfrentar este tipo de problemas y que la tecnología siempre va por delante de la ley. Por eso es mejor prevenir y usar Internet responsablemente", dice Juan Ignacio Zamora.

"Es importante que cuando uno está en horario laboral, Internet se use para cuestiones laborales. Las empresas deben desarrollar reglamentos y educar sobre el uso correcto del Internet durante el espacio laboral. Son muchos los casos en que un mal uso de los recursos por parte de los empleados pone en riesgo los datos de la empresa", explicó el especialista.

Estos reglamentos deberán regular, principalmente, el uso de las redes sociales, el acceso a páginas indebidas y el correo electrónico. Roberto Lemaitre coincide con Zamora y agrega que las empresas también deben darle una participación más activa a las unidades tecnológicas al momento de tomar decisiones, ya que de eso dependerá, en gran medida, la seguridad de los datos empresariales.

"Las empresas definitivamente no pueden dejar de actualizar su tecnología, pero para hacer la implementación tecnológica deben contar con equipos especializados en el tema de ciberseguridad y que estos tengan participación directa en la toma de decisiones. Cerca de la gerencia debe haber alguien que maneje estos temas y que haga que las empresas estén más seguras", comenta el abogado.

Pese a los esfuerzos tanto nacionales como internacionales para regular los usos indebidos que se le da a Internet, ambos especialistas consideran que buena parte del esfuerzo de la sociedad debe pasar por desarrollar usuarios con una mayor cultura digital.

Esa mejora en la cultura digital se logra, según Lemaitre, con prácticas tan básicas como leer las condiciones antes de instalar una aplicación, utilizar contraseñas más seguras y emplear las redes sociales en forma responsable. Empezar con esos pequeños cambios sería la clave para enfrentar los retos que nos plantea Internet, una tecnología que está presente en la mayoría de campos de la actualidad.