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.