UNIVERSIDAD DE COSTA RICA

Abogados analizan delitos informáticos

Desconocimiento y vacíos legales facilitan la ciberdelincuencia en el país

4 OCT 2011 Sociedad

El Lic. Roberto Lemaitre Picado es abogado e ingeniero informático. Recientemente publicó el libro "Manual sobre delitos informáticos para la cibersociedad costarricense" (foto Laura Rodríguez Rodríguez).

El desconocimiento que tienen los usuarios de Internet sobre los ataques informáticos, así como los vacíos en la legislación costarricense, facilitan el ser víctima de la ciberdelincuencia. Esta fue la principal conclusión de la mesa redonda ***Los delitos informáticos en Costa Rica***, la cual contó con la participación de diferentes especialistas en derecho.

“Delito informático es aquella acción típica, antijurídica y culpable realizada por medios informáticos o cuya acción por modificar los datos a un dispositivo”, definió el abogado e ingeniero informático, Lic. Roberto Lemaitre Picado, quien forma parte del Área de Informática Jurídica de la Facultad de Derecho de la Universidad de Costa Rica.

El Lic. Lemaitre explicó que actualmente Internet es considerado un mundo enorme y complejo, donde pueden ocurrir delitos informáticos debido a la facilidad con la que se comparten datos e información en tiempo real. A esto se le suma que **los usuarios de la red no están conscientes de los peligros a los cuales se exponen**, con lo que aumenta el riesgo de ser víctima de un ataque.

En la Internet no sólo se puede encontrar software malintencionado, sino que también ocurre la suplantación de identidad, recolección de información privada de redes sociales y ataques multiplataformas. El uso de *software* sin una licencia del fabricante, también impide que se instalen actualizaciones que protegen la seguridad de los sistemas. Los delitos ya no se limitan a las computadoras, sino que **incluyen a todo dispositivo que tenga conexión a Internet** como los celulares y las tabletas, explicó el Lic. Lemaitre.

Por ejemplo, el abogado citó el Reporte de Seguridad Informática 2011 de la empresa ESET, el cual indica que en Costa Rica, el 36% de las empresas permite el uso de redes sociales sin ninguna restricción. El 50% de los usuarios costarricenses considera que no hay *malware* (software malicioso) en dichos sitios, y el 22% agrega como contacto a personas desconocidas.

El Dr. Carlos Chinchilla Sandí es Magistrado de la Sala III de la Corte Suprema de Justicia, egresado de la UCR y cuenta con publicaciones sobre delitos informáticos y derecho penal (foto Laura Rodríguez).

Otro de los participantes, el Dr. Carlos Chinchilla Sandí, Magistrado de la Sala III de lo Penal y egresado de Derecho de la UCR, también coincidió en que **los usuarios creen que no serán víctimas de un ataque cibernético en Internet, especialmente en las redes sociales.**

Quien comete un delito informático puede ser una persona o un grupo de personas que manejan información sensible o importante, hasta profesionales especializados en informática. El Dr. Chinchilla, explicó que **las personas que delinquen en la red se muestran agradables, amigables y educadas**, por lo que la víctima no sospecha que está frente a un ataque informático.

La persecución y la prueba de un delito informático son complicadas. Por ejemplo, un *ciberdelincuente* puede atacar desde Costa Rica y hacer creer que el delito se cometió en cualquier otro país del mundo, lo que dificulta la captura física del atacante y se requiere de colaboración internacional. Muchas empresas no denuncian que sus sistemas son víctimas de ataques informáticos, por miedo a dañar su imagen y perder la confianza de sus clientes, lo que colabora con la impunidad, comentó el Lic. Lemaitre.

Marco jurídico costarricense y delitos informáticos

El M.Sc. Francisco Salas Ruiz es profesor de la Facultad de Derecho de la UCR y ha representado a Costa Rica en diferentes comisiones sobre delitos informáticos fuera del país (foto Laura Rodríguez Rodríguez).

Los especialistas participantes en esta mesa redonda coincidieron en que la legislación costarricense presenta serias deficiencias para proteger a la ciudadanía de la ciberdelincuencia, debido a los **vacíos conceptuales y la falta de tipos penales para sancionar.**

El Dr. Chinchilla explicó que en los sistemas informáticos hay tres fases importantes: el ingreso, procesamiento y salida de información. Está comprobado estadísticamente, que el 85% de los ataques cibernéticos ocurren en la primera etapa, sin embargo, en la ley penal actual sólo se contemplan el procesamiento y la salida de datos. Los delitos informáticos se tipifican en los artículos 196 bis, 217 bis y 229 bis del Código Penal costarricense, los cuales tratan sobre violación a comunicaciones electrónicas, fraude informático, alteración de datos y sabotaje.

Los expositores también plantearon que otro de los vacíos de la legislación costarricense en materia de *ciberdelitos*, es que en ésta **sólo se contemplan sanciones a personas físicas, y no a empresas que comentan actos ilícitos,** con lo que se facilita el crimen organizado. Además, las penas por los delitos informáticos se consideran muy cortas, pues van de los seis meses a los seis años de cárcel.

"Muchos de los delitos de carácter informático son delitos de peligro. Por lo tanto, no necesitamos ver resultados para sancionarlos como tales. Además son delitos de carácter patrimonial que dañan a muchas personas", calificó el Dr. Chinchilla.

El público asistente a la mesa redonda mostró interés y preocupación por la alta vulnerabilidad de sufrir un ataque informático (foto Laura Rodríguez Rodríguez).

La buena noticia es que existe **un proyecto de ley más completo sobre esta materia en la Asamblea Legislativa.** El diputado y jefe de fracción del partido Movimiento Libertario, Lic. Danilo Cubero Corrales, expuso que el proyecto ha pasado por diferentes reformas y consultas constitucionales desde que se planteó en el 2009. Actualmente está en el lugar 28 del orden del día de la agenda legislativa para ser discutido y votado en el plenario.

Según el Dr. Chinchilla, **este proyecto de ley se puede calificar como pionero en la región y garantiza mayor protección** que la legislación actual. "Esta propuesta de reforma legislativa sobre los delitos informáticos es realmente una legislación de primer mundo, que muchos países ni siquiera tienen, y está puesta en beneficio de un país latinoamericano".

La nueva ley incluye más tipos penales como violación de correspondencia y comunicaciones, violación de datos personales, hurto agravado, suplantación de identidad, estafa informática, espionaje informático, hurto de virus, software malicioso, clonación de páginas electrónicas y páginas web, suplantación de sitios web para recopilar datos personales, técnicas de *pharming* y *phising*, fraude informático y sabotaje informático.

Si bien Costa Rica está cerca de aprobar una legislación avanzada, el Procurador del Sistema Nacional de Legislación Vigente y docente en la UCR, M.Sc. Francisco Salas Ruiz, destacó la necesidad de que el país se una al Convenio de Europa sobre ciberdelincuencia. Una vez que el país esté suscrito, podrá pedir ayuda a otros países que forman parte del convenio para perseguir los delitos informáticos.

Los especialistas, fueron enfáticos al decir que **el derecho informático requiere de un trabajo interdisciplinario** que incluya a juristas y especialistas en informática y computación. Además, **la legislación necesita una actualización constante**, tal y cómo lo hace la tecnología.

“Para comprender el delito informático es necesario conocer las redes informáticas y los equipos informáticos. Un delito como este no se visualiza correctamente si no se comprende el ecosistema en el que se desarrolla”, concluyó el Lic. Lemaitre. También es necesario que en Costa Rica se cree una institución especializada en el sector judicial que se encargue de investigar los delitos informáticos, observó el abogado.

Esta mesa redonda, fue organizada por la Facultad de Derecho de la Universidad de Costa Rica, en conjunto con el Departamento de Servicios Bibliotecarios, Documentación e Información de la Asamblea Legislativa. Fue moderada por el decano de dicha facultad, el Dr. Daniel Gadea Nieto.

Anna Georgina Velásquez Vásquez
Periodista Oficina de Divulgación e Información
anna.velasquez@ucr.ac.cr

Etiquetas: facultad de derecho, delitos informaticos, ciberdelincuencia.