UNIVERSIDAD DE COSTA RICA

Especialistas reconocen necesidad de ley sobre *ciberdelitos*

23 OCT 2009

1. El Dr. Christian Hess hizo énfasis en la necesidad de crear una jurisdicción específica para regular la delincuencia informática, en las jornadas sobre Delitos Informáticos y Ciberseguridad. (Foto: Luis Alvarado)

Especialistas en derecho discutieron las características de los delitos informáticos y las posibles soluciones normativas para combatirlos en el foro *Tipo y naturaleza de los ciberdelitos*, que se llevó a cabo como parte de unas jornadas organizadas por el Programa Sociedad de la Información y el Conocimiento (Prosic) de la Universidad de Costa Rica (UCR).

El foro contó con dos paneles de discusión en los que presentaron sus ponencias distintos especialistas en materia de delincuencia informática.

Por su parte, el Dr. Christian Hess Araya, Juez del Poder Judicial, explicó que la forma de abordar esta temática se da desde dos tendencias: la que considera los delitos informáticos como conductas novedosas, en cuyo caso las acciones y los tipos penales son nuevos y múltiples; y la que ve esos delitos como conductas tradicionales en un contexto moderno, para los cuales se reforman o agregan leyes existentes.

En el caso de Costa Rica se han utilizado ambas tendencias, en una combinación de reformas y creación de tipos penales, que castigan las acciones delictivas, por ejemplo la creación de los **delitos de fraude electrónico, alteración de datos y sabotaje informático** y la propuesta para reformar artículos del Código Penal, en cuanto a fraudes de tarjetas de crédito e información bancaria o el proyecto de Ley de Delitos Informáticos.

El Lic. Erick Lewis Hernández, jefe de Delitos Informáticos del Organismo de Investigación Judicial, manifestó que en Costa Rica la delincuencia informática se da de dos formas principalmente: **la violación de comunicaciones electrónicas**, por medio del reenvío a cuentas ajenas y robo de claves de acceso a correos electrónicos y por **alteración de datos y sabotaje informático**, como el acceso a entidades públicas, la venta de información confidencial, el daño a la compra de equipos personales y el cambio de saldos de las cuentas bancarias.

El expositor comentó que existen otras formas de delincuencia recurrentes como son: **la producción y difusión de pornografía infantil, el acoso infantil, el robo de identidad, amenazas y extorsiones, estafas, fraudes y ciberterrorismo.**

El Dr. Carlos Chinchilla Sandí explicó que la delincuencia informática tiene relación directa con el derecho penal económico y de peligro, pues no requiere que la acción tenga efectos, basta con que induzca al peligro para que sea sancionada. (Foto: Luis Alvarado)

Los participantes destacaron la necesidad de integrar un enfoque judicial a uno educativo en materia de delincuencia informática. “No es un tema que se resuelva creando leyes, se requiere educación al público, sobre el uso correcto y seguro de la tecnología”, manifestó Hess.

Para la Licda. Adriana Rojas Rivero, presidenta de la Asociación de Consumidores Libres, la educación de los usuarios debe ir dirigida a solucionar la ingenuidad de las personas, enseñarles a no abrir correos de personas desconocidas, no seguir los vínculos a los sitios web de los bancos e informarse en un vocabulario no técnico ni especializado. Señaló que el seguro que proteja contra el fraude informático es una necesidad en Costa Rica.

Normativa internacional

El Lic. Francisco Salas Ruiz, Procurador Adjunto de Derechos Informáticos, hizo énfasis en la existencia de una normativa europea en cuanto a delitos informáticos, que entró en vigencia en julio de 2004. Esta norma, denominada Convención Europea sobre ciberdelincuencia, aporta definiciones sustantivas respecto a los términos utilizados como acciones delictivas y las características para su comisión.

Los participantes destacaron la apertura de esta normativa a la adhesión de países no pertenecientes al continente, como es el caso de Estados Unidos, Japón, Canadá y Sudáfrica; y Costa Rica, México, Chile y República Dominicana han sido invitados a adherirse.

Salas destaca la inclusión de normas que garantizan la integridad del usuario y el respeto a los derechos de propiedad intelectual y contempla acciones como la falsedad informática y la pornografía infantil, como delitos punibles.

Según la M.Sc. Georgina García Rojas, los derechos de propiedad intelectual son vulnerados en la delincuencia informática, pues Internet facilita los medios para su violación. (Foto: Luis Alvarado)

La legislación costarricense contiene normativa respecto a algunos de esos aspectos, pero adolece de normativa que garantice el respeto a los derechos de los usuarios.

Naturaleza jurídica

En cuanto a la naturaleza de los delitos informáticos, Hess explicó que se caracterizan por su dificultad de persecución, es decir "lo difícil que es identificar la comisión de un delito, identificar al autor o autores de ese delito, perseguirlos, o sea someterlos a la acción de la justicia y, eventualmente, condenarlos".

El Dr. Carlos Chinchilla Sandí, magistrado de la Sala Tercera, coincide con Hess en adjudicar esa cualidad a ese tipo de delitos. Según expresaron ambos, **destacan en su comisión la velocidad con la que se realizan, la distancia geográfica entre los sujetos involucrados debido al medio, que es Internet, la facilidad de encubrir las pruebas, el temor a denunciarlos y el perfil no tradicional del delincuente informático**.

Al respecto, Adriana Rojas expresó que delitos informáticos son las violaciones a los derechos de autor, el robo de datos privados, la pornografía infantil y el fraude electrónico, por ejemplo, y no aquellos que se cometan sobre artefactos tecnológicos, como sería robar un cajero automático.

Hess agregó que un aspecto fundamental que impide el castigo de los delincuentes informáticos es la indiferencia de la opinión pública, esto porque no se le da trascendencia a este tipo de delitos, como sí se hace a los tradicionales.

Rojas opina que por desconocimiento y confusión, generalmente, no se realizan las denuncias correspondientes, mientras Carlos Chinchilla, se lo achaca al temor, al desprestigio y la consecuente pérdida económica, todo lo cual se convierte en una de las más grandes trabas a la penalización de los delitos informáticos.

En el foro también participaron la M.Sc. Georgina García Rojas, asesora de la Asamblea Legislativa, el M.Sc. Iván Salas Leitón, del Observatorio de la Libertad de Expresión de la UCR y la Licda. Rocío Cerdas Quesada, tesorera del Colegio de Abogados.

Terminología de los ciberdelitos

Delitos informáticos: **Acción delictiva que realiza una persona con la utilización de un medio informático, lesionado los derechos del titular de un elemento informático, ya sean máquinas (hardware) o programas (software).**

Virus informático: **programa que tiene por objetivo alterar el funcionamiento normal del equipo de cómputo, sin autorización del usuario.**

Spyware: **programa que se instala en el equipo de cómputo, con el fin de recopilar información sobre las actividades que se realizan en él.**

Phishing: **tipo de estafa que utiliza medios electrónicos e informáticos para obtener información confidencial de forma engañosa, como claves de acceso o información bancaria.**

Pharming: **basado en ingeniería social, la víctima es conducida a un sitio falso para que ceda su información confidencial y luego es redirigida a un sitio falso, con un nombre igual al sitio de destino.**

Keylogger: programa espía que guarda las teclas presionadas en el teclado y hace que el correo electrónico lleve un archivo que tiene el programa escondido para transmitir las claves.

Mayela Castillo Villachica.
Periodista Oficina de Divulgación e Información
mayela.castillo@ucr.ac.cr