ASAMBLEA LEGISLATIVA DE LA
REPÚBLICA DE COSTA RICA

PROYECTO DE LEY

REFORMA DEL ARTÍCULO 229 BIS DEL CÓDIGO PENAL Y ADICIÓN DE UN NUEVO CAPÍTULO DENOMINADO DELITOS INFORMÁTICOS

LUIS ANTONIO BARRANTES CASTRO
DIPUTADO

EXPEDIENTE N.º 17.613

DEPARTAMENTO DE SERVICIOS
PARLAMENTARIOS

PROYECTO DE LEY

REFORMA DEL ARTÍCULO 229 BIS DEL CÓDIGO PENAL Y ADICIÓN DE UN NUEVO CAPÍTULO DENOMINADO DELITOS INFORMÁTICOS

Expediente N.º 17.613

ASAMBLEA LEGISLATIVA:

En la última década, el tema de seguridad ciudadana ha empezado a tomar especial relevancia en la sociedad costarricense, al punto de ser tema de discusión al mismo nivel que la educación y la salud pública. El motivo de esta situación, no solo lo es el aumento desmedido de la delincuencia sino la sofisticación de los métodos que aplican los antisociales para perjudicar tanto la integridad física y moral así como el patrimonio de los ciudadanos.

Se puede definir como delito informático como *"crimen genérico o crimen electrónico, que agobia con operaciones ilícitas realizadas por medio de pcs o del Internet o que tienen como objetivo destruir y dañar ordenadores, medios electrónicos y redes de Internet. Sin embargo, las categorías que definen un delito informático son aún mayores y complejas y pueden incluir delitos tradicionales como el fraude, el robo, chantaje, falsificación y la malversación de caudales públicos en los cuales ordenadores y redes han sido utilizados. Con el desarrollo de la programación y de Internet, los delitos informáticos se han vuelto más frecuentes y sofisticados.*

Existen actividades delictivas que se realizan por medio de estructuras electrónicas que van ligadas a un sinnúmero de herramientas delictivas que buscan infringir y dañar todo lo que encuentren en el ámbito informático: ingreso ilegal a sistemas, interceptado ilegal de redes, interferencias, daños en la información (borrado, dañado, alteración o supresión de datacredito), mal uso de artefactos, chantajes, fraude electrónico, ataques a sistemas, robo de bancos, ataques realizados por hackers, violación de los derechos de autor, pornografía infantil, pedofilia en Internet, violación de información confidencial y muchos otros."[1]

Un ejemplo de la sofisticación de estos métodos, es el aumento de los llamados delitos informáticos; según indicó el Organismo de Investigación Judicial por medio de un comunicado de prensa, al 4 de mayo de 2009[2] aproximadamente 25 personas habían sido estafadas por medio de delitos informáticos a través de

[1] http://es.wikipedia.org/wiki/Delito_inform%C3%A1tico.
[2] www.prensalibre.cr. Andrey Berrocal, martes 5 de mayo de 2009.

las campañas publicitarias de los bancos estatales, en donde las víctimas revelaban sus cuentas por Internet.

El 5 de mayo del 2009, en La Prensa Libre se explica "*que este tipo de delitos sólo los cometen quienes conocen las técnicas para hacerlo y cuentan con los equipos especiales.*

Dos de los métodos más usados en Costa Rica son el Phishing y el Pharming. El primero consiste en enviar un correo electrónico a la víctima, el cual proviene de un ente oficial, pero en realidad es falso, y en cuyo contenido se hace una solicitud expresa para actualizar la información confidencial perteneciente al cliente, como el nombre de usuario, contraseña, número de tarjeta y PIN entre otros, los cuales al final terminan en las computadoras de los estafadores.

La segunda técnica conocida como Pharming, es cuando mediante la alteración del Servidor de DNS de un Proveedor de Servicios de Internet (Racsa, ICE), y del DNS del Sistema Operativo de la computadora de un usuario. En este caso, es posible a través de la introducción de un programa malicioso, modificar el archivo de nombre hosts para el caso del Sistema Operativo Windows. Estos programas pueden provenir de correos electrónicos, descargas por Internet o medios de almacenamiento externos como llaves USB, entre otros.

Luego de acceder al vínculo referenciado en la página de Internet enviada, se ejecuta el programa malicioso, el cual modificará el archivo hosts de la computadora del usuario, sin su conocimiento, quien finalmente luego de digitar las direcciones de Internet en su navegador será redireccionado a una página de Internet fraudulenta.

Las autoridades, de momento, recomiendan a los clientes bancarios no abrir correos de remitentes desconocidos".

Los actos ilegales realizados a partir de la tecnología, no se habían tipificado como delitos hasta hace poco en nuestro país; empero, el avance de un campo tan vasto como el de la informática, si por un lado ha permitido el crecimiento tecnológico y económico de la sociedad, por otro lado, paradójicamente, ha venido a significar el instrumento idóneo para menoscabar el patrimonio económico de personas e instituciones. Quizá hasta hace poco no se consideraba necesario resguardar el bien jurídico de la información; sin embargo, actualmente es completamente evidente la relevancia de hacerlo ya que con estos delitos se ven comprometidos otros bienes jurídicos tutelados como el patrimonio o la protección de datos personales, entre muchos otros.

Es por esto que en aras de penalizar acciones y tutelar el bien jurídico de la información y generar herramientas eficientes y eficaces para condenar delitos informáticos que afectan cada vez más el patrimonio de los costarricenses, se presenta el siguiente proyecto de ley.

LA ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE COSTA RICA
DECRETA:

REFORMA DEL ARTÍCULO 229 BIS DEL CÓDIGO PENAL Y ADICIÓN DE UN NUEVO CAPÍTULO DENOMINADO DELITOS INFORMÁTICOS

ARTÍCULO 1.- Refórmase el artículo 229 bis del Código Penal, Ley N.° 4573 y sus reformas.

"Artículo 229 bis.-

Daño informático

Se impondrá pena de prisión de tres a seis años al que por cualquier medio accese, borre, suprima, modifique o inutilice, sin autorización, los datos registrados en una computadora."

ARTÍCULO 2.- Adiciónase un capítulo nuevo al Código Penal, Ley N.º 4573 y sus reformas.

"CAPÍTULO ___
DELITOS INFORMÁTICOS

ARTÍCULO NUEVO
Abuso de medios informáticos

Será sancionado con la pena de tres a seis años de prisión, el que sin autorización o cediendo la que se le hubiere concedido, con el fin de procurar un beneficio indebido para sí o para un tercero, intercepte, interfiere, use o permita que otra use un sistema o red de computadoras o de telecomunicaciones, un programa de computación o de telecomunicaciones, un soporte lógico, un programa de computación o una base de datos, o cualquier otra aplicación informática, de telecomunicaciones o telemática.

ARTÍCULO NUEVO
Suplantación de identidad

Será sancionado con pena de prisión de tres a seis años, aquel que utilizando la identidad de otra persona, se haga pasar por esta, en cualquier red social.

ARTÍCULO NUEVO
Estafa informática

Se impondrá prisión de tres a doce años a la persona que, con la intención de procurar u obtener un beneficio patrimonial para sí o para un tercero, influya o manipule el ingreso, procesamiento o el resultado de los datos de un sistema de cómputo, mediante programación, empleo de datos falsos o incompletos, uso indebido de datos o cualquier otra acción que incida en el proceso de los datos del sistema.

ARTÍCULO NUEVO
Espionaje informático

Se impondrá prisión de tres a seis años al que se apodere, interfiera, transmita, copie, modifique, destruya, utilice, impida, o recicle datos de valor para el tráfico económico de la industria y el comercio. La pena se aumentará en un tercio si son datos de carácter político, relacionados con la seguridad del Estado.

ARTÍCULO NUEVO
Uso de virus (software malicioso)

Se impondrá pena de tres a seis años de prisión *al que produzca, trafique,* adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional virus (software malicioso), u otro programa de computación de efectos dañinos.

ARTÍCULO NUEVO
Clonación de páginas electrónicas (páginas web)

Se impondrá prisión de tres a seis años siempre que no se trate de una conducta sancionada con una pena más grave, al que diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas clonadas de una original previamente existente.

ARTÍCULO NUEVO
Suplantación de sitios web para capturar datos personales (phishing y pharming 0)

Se impondrá pena de prisión de tres a seis años y multas de 200 a 1000 salarios bases siempre que la conducta no constituya delito sancionado con pena más grave, al que diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas (web side), CLONADAS DE UNA ORIGINAL PREVIAMENTE EXISTENTE, enlaces (links) o ventanas emergentes (pop up), con la finalidad de inducir, convencer a los consumidores o divulgar información personal o financiera, modifique el sistema de resolución de nombres de dominio, lo que hace al usuario

ingresar a una IP diferente en la creencia de que está accediendo a su banco u otro sitio personal o de confianza.

ARTÍCULO NUEVO
Sabotaje informático

Se impondrá pena de tres a seis años de prisión, al que destruya, altere, entorpezca o inutilice un sistema de tratamiento de información, sus partes o componentes lógicos, una base de datos o un sistema informático, o impida, altere, obstaculice o modifique su funcionamiento sin autorización.

La pena será de prisión de cuatro a ocho años, cuando:

a) Como consecuencia de la conducta del autor sobreviniere peligro o daño común. Siempre que la conducta no se encuentre más severamente sancionada.
b) Si la conducta se realizare en provecho propio o de un tercero, por parte de empleado o contratista del sistema informático o telemático o por un servidor público.
c) Si contienen datos de carácter público.

El que emplee medios tecnológicos que impidan a personas autorizadas acceder a la utilización lícita de los sistemas o redes de telecomunicaciones, sin estar facultado."

Rige a partir de su publicación.

Luis Antonio Barrantes Castro
DIPUTADO

15 de febrero de 2009.

NOTA: Este proyecto pasó a estudio e informe de la Comisión Especial de Seguridad Ciudadana.