Inter Sedes. Vol. VIII. (14-2007) 49-64. ISSN: 1409-4746

ALCANCE DE LA LEGISLACIÓN COSTARRICENSE EN MATERIA DE DELITOS INFORMÁTICOS: UN ANÁLISIS PRELIMINAR

Susan Chen Mok[*]

Recepción: 3 de agosto de 2007 • Aprobación: 8 de febrero de 2008

RESUMEN

El artículo aborda la problemática de las actividades ilegales que se desarrolla en la Internet, haciendo un análisis del alcance de la legislación costarricense para regular esta materia. Para ello se presenta la problemática, se revisa la normativa y se analiza el alcance de la legislación actual.

Palabras claves: Internet, legislación, delito informático.

ABSTRACT

This article underlines the problems regarding the illegal activity to get in Internet. It analyses the scope of the Costa Rican law on this matter by outlining the problem, then the available regulation is reviewed, and finally, the scope of the law is analyzed.

Key Words: Internet, legislation, computer offense.

* Profesora de la Sede del Pacífico de la Universidad de Costa Rica [susan.chen@ucr.ac.cr / schen64@gmail.com]

Introducción

El desarrollo de las tecnologías de información y comunicación ha ampliado de forma inimaginable las posibilidades de negocios, e igualmente, ha facilitado la comisión de gran variedad de delitos, entre los que se encuentran los de tipo fiscal, penal, comercial, civil y aduanero entre otros, y Costa Rica no está exenta de ello.

En el país se abrió la Unidad de Delitos Informáticos del Organismo de Investigación Judicial en el año 1996, a partir del cual y hasta el año 2001, habían recibido alrededor de 300 casos, un promedio de 60 ilícitos cada año, según informa Solano (2001) en un artículo publicado en el periódico La Nación del 1 de junio de 2001. De acuerdo con Lewis (2006), en el año 2004 se reportaron 134 denuncias y en el 2005, 142 denuncias. Lo que muestra una tendencia de aumento en este tipo de delitos.

Lo anterior hace necesario analizar el panorama actual del marco legal existente en Costa Rica, con el fin de que sirva de base para el desarrollo de un marco general para el inicio de un estudio más exhaustivo de las posibles carencias que presente el aparato legal costarricense con relación al desarrollo de las tecnologías de información y comunicación.

Este trabajo de investigación tiene como objetivo estudiar la situación legal costarricense con el fin de determinar su alcance para regular la materia relacionada con los delitos que pueden cometerse a través de la Red y presentar un panorama general de la situación del país en este ámbito. Se limita al análisis de la legislación existente en Costa Rica en materia de delitos informáticos.

Para hacer el análisis del alcance de la legislación actual, se presenta primero el tema relacionado con la materia que debe ser regulada y la legislación existente, e inmediatamente se aborda al análisis de la situación legal respectiva.

El concepto

El uso y desarrollo de la informática se ha ampliado a todos los campos del saber y en casi todos los países. Todas las administraciones, industrias, organizaciones, así como la investigación científica e incluso el estudio y el ocio se han visto impactadas por el uso de las tecnologías de información y comunicación. Hoy en día es casi imposible concebir algún proceso sin pensar en el uso de la informática. Sin embargo, junto a las incuestionables ventajas que presenta, comienzan a surgir aspectos negativos, como por ejemplo los delitos informáticos.

El desarrollo de las tecnologías de información y comunicación ha abierto nuevas posibilidades de delincuencia antes desconocidas. Se encuentran hoy posibilidades de cometer actos ilícitos de manera muy fácil y sin ser descubiertos, fácilmente se manipulan los sistemas de información con ánimo de lucro, así como se destruyen los programas informáticos o datos. Es posible tener acceso y utilización indebida de la información, que puede afectar la esfera de la privacidad de los individuos. Todos estos aspectos están relacionados con el procesamiento electrónico de los datos mediante los cuales es posible obtener grandes beneficios económicos o causar daños materiales o morales importantes.

Y como lo indica Téllez (2004), no sólo la cuantía de los perjuicios así ocasionados

es a menudo infinitamente superior a la que es usual en la delincuencia tradicional, sino que también son mucho más elevadas las posibilidades de que no lleguen a descubrirse. Se trata de una delincuencia de especialistas capaces muchas veces de borrar toda huella de los hechos.

De acuerdo con Téllez (2004), la informática puede ser el objeto del ataque o el medio para cometer otros delitos. La informática reúne unas características como: la gran cantidad de datos que se acumulan, la facilidad de acceso a ellos y la relativamente fácil manipulación de los datos; que la convierten en un medio idóneo para la comisión de muy distintas modalidades delictivas.

Por otro lado, el desarrollo de Internet junto con el desarrollo de los sistemas informáticos ha facilitado y ampliado las posibilidades para la comisión de los delitos.

Según Téllez Valdez (2004), los delitos informáticos presentan las siguientes características principales:

- Son conductas criminales de cuello blanco (white collar crime), en tanto que sólo un determinado número de personas con ciertos conocimientos (en este caso técnicos) pueden llegar a cometerlas.
- Son acciones ocupacionales, en cuanto a que muchas veces se realizan cuando el sujeto se halla trabajando.
- Son acciones de oportunidad, ya que se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico.
- Provocan serias pérdidas económicas, ya que casi siempre producen "beneficios" de más de cinco cifras a aquellos que las realizan.
- Ofrecen posibilidades de tiempo y espacio, ya que en milésimas de segundo y sin una necesaria presencia física pueden llegar a consumarse.
- Son muchos los casos y pocas las denuncias, y todo ello debido a la misma falta de regulación por parte del Derecho.
- Son muy sofisticados y relativamente frecuentes en el ámbito militar.
- Presentan grandes dificultades para su comprobación, esto por su mismo carácter técnico.
- En su mayoría son imprudenciales y no necesariamente se cometen con intención.
- Ofrecen facilidades para su comisión a los menores de edad.
- Tienden a proliferar cada vez más, por lo que requieren una urgente regulación.
- Por el momento siguen siendo ilícitos impunes de manera manifiesta ante la ley.

En los siguientes apartados se analizará la situación legislativa de Costa Rica de algunos de los delitos informáticos tipificados.

Fraude informático

El establecimiento del Fraude Informático como delito fue "la reforma más relevante en materia de criminalidad informática...." de acuerdo con Chinchilla (2002: 110). Este es el delito informático más difundido.

Según Echegaray (2001):

> en la estafa informática no se ejerce violencia en las personas ni fuerza en las cosas, hay una manipulación informática y como consecuencia de ello, al igual que en el hurto, se produce una transferencia,

una sustracción, un apoderamiento sin el consentimiento de su dueño (97).

El fraude informático puede ser cubierto por el artículo 217 bis de la Ley 8148, que reza así:

Artículo 217 bis.- Fraude informático

Se impondrá pena de prisión de uno a diez años a la persona que, con la intención de procurar u obtener un beneficio patrimonial para sí o para un tercero, influya en el 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. (Asamblea Legislativa de CR, 2001-b: 2).

La frase "o cualquier otra acción" del artículo 217 bis podría generar problema de inconstitucionalidad pues no individualiza las acciones penadas por ley requisito para la Ley Penal.

Además, el problema es determinar y ubicar al infractor en el ambiente de Internet, no hay norma que permita juzgar en el exterior o podría ocurrir que no pueda llevarse a cabo la extradición, por lo que el delito quedaría impune.

Sabotaje en la Red

El artículo 217 bis de la Ley 8148 impone una pena de uno a diez años a la persona que procura obtener un beneficio patrimonial para sí o para un tercero, influyendo en el 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.

La estafa pretende que la manipulación genere una alteración del sistema que permita realizar una maniobra, con el fin de obtener un beneficio patrimonial para sí o para un tercero.

Sin embargo, el delincuente informático que inserta un virus en una computadora de un banco, genera un perjuicio patrimonial, aunque su dolo no es favorecerse de este perjuicio ni de otro, su finalidad es probar un virus o sus habilidades para crearlos.

De acuerdo con Salas y Sánchez (1999), "la actividad criminal consiste en el acceso directo u oculto no autorizado a un sistema informático mediante la introducción de nuevos programas denominados virus, gusanos o bombas lógicas" (189).

Estas manipulaciones se caracterizan principalmente por ser realizadas desde fuera del lugar en que se encuentra el computador afectado, incluso puede ser desde otra parte del mundo.

Para estos casos, donde el fin no es obtener ningún beneficio propio ni para un tercero, pero sí causan daños materiales, pueden calzar en el tipo penal de delito de alteración de datos y sabotaje informático, y aplicarse el artículo 229 bis.

Artículo 229 bis.- Alteración de datos y sabotaje informático

Se impondrá pena de prisión de uno a cuatro años a la persona que por cualquier medio acceda, borre, suprima, modifique o inutilice sin autorización los datos registrados en una computadora. (Asamblea Legislativa de CR, 2001-b: 2).

Este artículo crea el delito de alteración de datos y sabotaje informático, se refiere a la persona que por cualquier medio accede, borre, suprima, modifique o inutilice sin autorización los datos registrados en una computadora.

Se amplía el grupo de delitos para agregar los daños al elemento físico

portador de datos informáticos (disco o computadora), o en caso de que se produzca sabotaje contra los elementos lógicos del sistema, es decir, siempre que se destruyan datos, o al dar órdenes falsas se disminuya de cualquier manera la funcionalidad del sistema.

También se encuentran los artículos 221 y 222 de la Ley 7557 General de Aduanas que establece penas de prisión de uno a tres años al que accede, apodere, copie, destruya, inutilice, altere, facilite, transfiera o tenga en su poder, sin autorización de la autoridad aduanera, cualquier programa de computación y sus bases de datos, utilizados por el Servicio Nacional de Aduanas, siempre que hayan sido declarados de uso restringido por esta autoridad; también es sancionado si se daña componentes informáticos o se facilite clave de acceso; y en el caso agravado cuando es un funcionario o participen más tres o más personas.

En el mismo sentido y con la misma penalización se encuentra el artículo 111 de la Ley 8131 de Administración Financiera de la República y Presupuestos Públicos, cuando los actos se realizan contra los sistemas informáticos de la Administración Financiera y de Proveeduría.

Además se encuentra en la Ley 7535 de Justicia Tributaria, en la que se reforma los artículos del 90 al 98 del Código de Normas y Procedimientos Tributarios, y en la que se establece los delitos tributarios con penas de prisión de uno a diez años. Entre los delitos se encuentran:

- Ocultar o destruir información, libros contables, bienes, documentos, registros, sistemas y programas computarizados, soportes magnéticos u otros medios de trascendencia tributaria en las investigaciones y los procedimientos tributarios;
- Utilizar cualquier medio tecnológico para acceder a los sistemas de información o las bases de datos de la Administración Tributaria, sin la autorización correspondiente;
- Apoderar, copiar, destruir, inutilizar, alterar, transferir o tener en su poder, sin la autorización debida de la Administración Tributaria, cualquier programa de cómputo utilizado por ella para administrar la información tributaria y sus bases de datos;
- Facilitar la clave de acceso asignado para ingresar a los sistemas de información tributaria.

Observe que ya se consideraba en estas Leyes algunos delitos informáticos tipificados luego, de manera general para todas las situaciones, en la Ley 8148.

Al igual que el delito anterior, el problema es determinar y ubicar al infractor en el ambiente de Internet además de que no hay norma que permita juzgar en el exterior o podría ocurrir que no pueda llevarse a cabo la extradición, por lo que el delito quedaría impune. Es necesario que los delitos informáticos tengan elementos comunes entre los diversos países, de forma tal que pueda haber una sanción eficaz cuando se cometen desde fuera del país.

Violación de comunicaciones electrónicas

La violación de las comunicaciones electrónicas se refiere al acceso y alteración no autorizados a los elementos electrónicos en donde se encuentra

almacenado los datos privados de una persona.

El Código Penal también incluye la violación de comunicaciones electrónica como un delito. El artículo 196 bis penaliza con seis meses a dos años al que vulnere la intimidad de otro. Es decir que sin su consentimiento se apodere, accese, modifique, altere, suprima, intercepte, interfiera, utilice, difunda o desvíe de su destino mensajes, datos e imágenes contenidas en medios electrónicos, informáticos, magnéticos y telemáticos. Y las penas serán de uno a tres años, si estas acciones son realizadas por los propios encargados de los soportes electrónicos, informáticos, magnéticos y telemáticos en donde se encuentra almacenado los datos.

El acceso no autorizado a datos personales o privados contenidos en medios electrónicos, informáticos, magnéticos y telemáticos tiene protección en el Código Penal costarricense con esta norma. Aunque no exista una Ley para la protección de datos personales, propiamente.

Un avance en Costa Rica en relación a una protección de datos personales más integral está en la presentación de un proyecto de Ley que se encuentra en la Asamblea Legislativa, el expediente 15178 Proyecto de Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales, que pasó a estudio a la Comisión Permanente de Asuntos Jurídicos, el 27 de marzo de 2003. Este proyecto de Ley es muy completo en materia de protección de datos personales y coloca al país a la altura de los países de la Unión Europea.

Igual que los anteriores, el problema es cuando se trata de una violación cometida por una persona que se encuentra en el extranjero. No se tiene mecanismos ágiles y eficientes para la extradición del infractor o puede ocurrir que no se pueda extraditar. Además de lo difícil que es determinar y ubicar al infractor aunque no se encuentre en el extranjero.

Todas estas conductas tienen en común la conexión telemática, por lo que se justifica, para efectos probatorios, que se amplíe la posibilidad de secuestrar documentos o recibir transmisiones en un número mayor de casos. El artículo 9 de la Ley sobre Registro, Secuestro y Examen de documentos privados e intervención de las comunicaciones, amplía la permisión de intervenir las telecomunicaciones digitales para esclarecer delitos.

ARTÍCULO 9.- Autorización de intervenciones

Dentro de los procedimientos de una investigación policial o jurisdiccional, los tribunales de justicia podrán autorizar la intervención de comunicaciones orales, escritas o de otro tipo, incluso las telecomunicaciones fijas, móviles, inalámbricas y digitales, cuando involucre el esclarecimiento de los siguientes delitos: secuestro extorsivo, corrupción agravada, proxenetismo agravado, fabricación o producción de pornografía, tráfico de personas y tráfico de personas para comercializar sus órganos; homicidio calificado; genocidio, terrorismo y los delitos previstos en la Ley sobre estupefacientes, sustancias psicotrópicas, drogas de uso no autorizado, legitimación de capitales y actividades conexas, Nº 8204, de 26 de diciembre de 2001.

En los mismos casos, dichos tribunales podrán autorizar la intervención de las comunicaciones entre los presentes, excepto lo dispuesto en el segundo párrafo del artículo 26 de la presente Ley; cuando se produzcan dentro de domicilios y recintos privados, la intervención solo podrá autorizarse si existen indicios suficientes de que se lleva a cabo una actividad delictiva.

(Este artículo 9, fue reformado por el artículo único de la Ley N° 8238, de 26 de marzo de 2002. Publicada en La Gaceta N° 74, de 18 de abril de 2002.) (Asamblea Legislativa, 2002: 1).

Falsificaciones de datos

La falsificación de datos en Internet como en cualquier medio informático encuentra una serie de problemas para ser comprendidos dentro de la figura tradicional de la falsificación de documentos del Código Penal de Costa Rica.

Del artículo 359 al 365 del Código Penal vigente tiene una concepción muy restringida de los requisitos del documento que ya no obedecen a las formas modernas de las relaciones jurídico-sociales.

En el Código Penal, el título XVI, delitos contra la fe pública, determina los tipos referentes a la falsificación de documento público o auténtico, la falsedad ideológica, la falsedad de documento privado, los documentos equiparados y certificados médicos.

La materialidad del documento, el concepto de documento y la manifestación de voluntad en el documento son tres asuntos que se deben analizar.

La materialidad entendida como atributos visuales o legibles hace que los documentos informáticos no formen parte del concepto de documento tal y como se entiende actualmente. Debería haber una referencia clara en el Código Penal al documento electrónico que puede ser sujeto de falsificación o alteración.

Ya existían en nuestro país muchos registros electrónicos que trabajan con originales en papel, pero que bien se podría decir que constituyen un documento público, como por ejemplo, el registrador que introduce al sistema de registro público una escritura de compraventa de un inmueble, está generando un documento público electrónico, pues para muchos consultantes bastará la consulta por computadora para realizar los trámites.

De acuerdo con Herrera (1999), el documento electrónico debe cumplir con dos aspectos: ser autorizado por un funcionario público (con los requisitos de investidura que esto implica), y otorgarse con las formalidades que la Ley exige (que debe crearse para solucionar el vacío).

Un requisito esencial en una escritura privada es la firma por parte de la persona de la cual proviene las declaraciones y que representa la conformidad de la voluntad de lo que aparece escrito en el documento. Aquí se entra a la discusión de la validez de la firma digital para asegurar la declaración y manifestación de voluntad en una transacción electrónica.

La manifestación de voluntad que contiene el documento puede ser alterada por datos falsos, por ejemplo, los casos en que se introducen al computador datos falsos o alterados que alteran los resultados de los programas informáticos a la hora de procesarlos. En este caso estamos frente a las defraudaciones. Ejemplo: girar una orden que saque una suma a cada salario y la ponga en una cuenta aparte. Esto es un delito puesto que por un lado se crea un dato informático falso (la nueva cuenta), y por otro lado se alteran varias cuentas existentes (las planillas de la empresa).

Dentro de la discusión de la falsificación de datos también se presenta el problema de la veracidad de la información contenida en Internet. Para resolver este problema se utilizan medios como la criptografía, las claves, y otros mecanismos de seguridad en la Red. La seguridad en las comunicaciones y transacciones requiere certeza principalmente en las de tipo financiero, inmobiliario, y personales entre otros.

Para la protección de las comunicaciones se utilizan protocolos que facilitan la confidencialidad en Internet. Entre ellos encontramos Secure Hipertex Transfer Protocol (SHTTP) para conexiones http, Secure Socket Layer (SSL) para comunicaciones encriptadas y con autenticación.

Un servidor seguro garantiza la confidencialidad de los datos personales que viajan por la red. El protocolo que se encarga de asegurar la privacidad de la información es el SSL. Este protocolo SSL encripta los datos que se envían a través de Internet, mediante el sistema RSA (algoritmo de encriptación). Los principales softwares para navegar Netscape y Explorer, actúan en colaboración con el servidor seguro. De tal forma que, cuando detectan que se encuentran en un servidor seguro, encriptan los datos de manera que resulta imposible que una persona ajena al circuito pueda acceder a su lectura.

Un servidor seguro se identifica mediante el símbolo de una Llave entera o un Candado cerrado, visible en los márgenes de la pantalla de la computadora. También se identifica un servidor seguro con un pequeño cambio en la descripción de la URL o dirección de la página . Por ejemplo la típica http se transforma en https.

También están los sistemas de claves, éstas hace uso de la criptografía para obtener transacciones seguras. La criptografía toma un texto, imagen o sonido no visible por los métodos convencionales y para hacerlo visible requiere de una clave para descifrar la codificación de la información. Solo el que tiene la clave puede descifrar la información. El método más eficaz en el campo del comercio electrónico es la utilización de criptografía asimétrica porque permite la transmisión de información a través de la red sin problemas de confidencialidad.

El otro problema es la veracidad del emisor, es decir, la seguridad de que el emisor es quien dice ser. Ante esta problemática surgen las terceras partes de confianza (entidades de certificación, Autoridades de Registro, Autoridades de fechado digital) y la firma digital.

Las terceras partes de confianza aseguran la transacción entre dos partes en una comunicación basada en la criptografía asimétrica, o también llamada de clave pública. Esta tecnología cuenta con dos claves, una denominada pública y otra privada. La primera se usa para otorgar a las demás personas para que envíen la información encriptada con esa clave, y sólo la puede descifrar el que tiene la clave privada, el propietario de la información, o el receptor autorizado.

El sistema de encriptación junto con la firma digital es el sistema más aceptado por los comerciantes y particulares para asegurar la información en la red. Se trata de un bloque de caracteres que acompaña el documento que el autor firma electrónicamente con la clave a la que solo él tiene acceso, cuya validez puede comprobarla el que tenga la clave pública del autor.

La ley 8454 contempla el concepto de documentos electrónicos, firma digital y entidades certificadoras de la problemática analizada. De acuerdo con Téramond y Fernández (2002), la firma digital le da seguridad a las transacciones electrónicas y su reconocimiento jurídico la equipararía a la firma manuscrita, con todos los derechos y deberes que tiene ésta.

> Por medio de la firma digital se logran las garantías necesarias para equiparar la firma digital con la manuscrita.....se garantiza la confidencialidad de la información intercambiada entre las partes (268).

El reconocimiento de la firma digital no crea ninguna nueva figura en el derecho, es una mera equiparación que conlleva las mismas consecuencias jurídicas de la firma manuscrita. Esto tiene importantes consecuencias para el reconocimiento del documento electrónico como un instrumento en términos jurídicos asegurándole, además, plenos efectos probatorios (269).

Por otro lado Monge y Murillo (2000) indican que:

el documento electrónico pertenece a la categoría de los documentos en sentido jurídico. Este tipo de documento cumple con los requisitos necesarios para ser presentado ante el órgano jurisdiccional: es representativo, pues representa un hecho; es declarativo, porque plasma la voluntad de las partes; y es un objeto mueble (190).

Por otro lado, la legislación costarricense tiene incorporado dentro de varias de sus leyes el término o concepto de documento electrónico desde mucho antes de que se promulgara la nueva Ley 8454: artículo 368 del Código Procesal Civil (Ley 7130); artículo 3 de la Ley del Sistema Nacional de Archivos (Ley 7202); artículo 1 de la Ley de Registro, Secuestro y Examen de documentos privados e intervención de las comunicaciones (Ley 7425); artículo 6 bis y 47 bis de la Ley Orgánica del Poder Judicial (Ley 7333), artículo 40 de la Ley de Contratación Administrativa y su Reglamento (Ley 7494); artículos 103 y 108 de la Ley General de Aduanas (Ley 7557).

La reciente promulgación de la Ley 8454 de Certificados, firmas digitales y documentos electrónicos en agosto de 2005 y su reglamento en marzo de 2006, resuelve el vacío existente sobre la validez y eficacia jurídica de los documentos electrónicos y firmas digitales. Sin embargo, Costa Rica todavía está en el proceso de implementar la Ley.

Además, la tecnología de criptografía asimétrica, firma electrónica, y entidades de certificación, permiten dar una alta seguridad a las transacciones electrónicas, sin embargo puede fallar, pues depende de la privacidad y seguridad con se administre la clave privada.

Usos de claves no autorizados

El acceso no autorizado se caracteriza por la intromisión en un sistema sin la debida aprobación de su titular o administrador. Por lo general se trata de acceso remoto al sistema, aspecto que se ve reforzado actualmente con Internet, donde priva este tipo de conexión, pero también ocurre en ambientes locales de Intranet.

La mayoría de los casos de accesos no autorizados se da cuando una clave privada es utilizada por una persona sin autorización del titular. En el artículo 221 de la Ley General de Aduanas (Ley 7557) está contemplado este tipo de delito e impone una pena de seis meses a un año si el empleado facilita la clave de acceso, pero solo se refiere al acceso a los sistemas informáticos de la Administración Aduanera.

De manera similar, el artículo 1 de la Ley 7535 en el que se reforman los artículo 96 y 97 del Código de Normas y Procedimientos Tributarios, sanciona el delito por prestar o facilitar la clave para acceder a los Sistema de Información Tributaria, con una pena de seis meses a cinco años de prisión.

El tema de las claves o "passwords" se tratan de manera indiferente en Costa Rica, se le resta importancia a la privacidad de éste.

A nivel mundial han sido numerosas las defraudaciones cometidas por la simple razón de que funcionarios públicos cedieran su clave a otra persona; incluso en las oficinas que trabajan con red, es común conocer la clave de los demás compañeros y hasta utilizar computadoras ajenas.

Se debe contemplar el tipo penal para estas actuaciones para ir protegiendo los sistemas que contienen información secreta (bancos, tribunales, tributación, presidencia, etc.). Los accesos no autorizados a través de claves es un delito informático que debe ser contemplado de manera más general, y no solo en los sistemas informáticos específicos, como los Sistemas de Administración Aduanera, o los Sistemas de Información Tributaria, como se encuentra actualmente.

Otros accesos no autorizados: el "hacker" o el "craker" en Internet

El "hacker" es la persona que realiza un acceso no autorizado a sistemas, ya sea con el fin de divertirse, probarse a sí mismos, o a otros, sus capacidades intelectuales. Por su parte, el "craker" es aquel que realiza un acceso no autorizado pero tienen la finalidad de destruir el sistema.

Los "hackers" lo hacen con la intención de aprender cómo funcionan los sistemas, su actividad se rige por la curiosidad. Pero aquí entra el tema del derecho a la intimidad y es necesario revisar si este tipo de acceso no autorizado debe ser contemplado como delito penal.

Lo que es preocupante es el tema del "craker", puesto que se han catalogados por algunos como vandalismo en el ciberespacio. Esta inseguridad se ha contrarrestado por medio de protecciones, las más comunes son las murallas de fuego ("firewalls") que consisten en estructuras de hardware o software que se colocan en la computadora y que funcionan como protección a intentos de accesos no autorizados. Se utiliza especialmente en computadoras programadas para controlar la conexión con Internet.

Las situaciones generadas por los "crakers" generan figuras de delitos ya tipificados, como lo son los daños al patrimonio, violación de programas, bases de datos, correspondencia, de los cuales ya se han referidos antes.

En el caso del hacker es necesario revisar si este tipo de acceso no autorizado debe ser contemplado como delito penal pues hay una invasión a la intimidad, el problema es que en Costa Rica no hay una Ley de Protección de Datos Personales, sólo lo establecido en la norma Constitucional en su artículo 24 (Rivera, 2003):

> Se garantiza el derecho a la intimidad, a la libertad y al secreto de las comunicaciones.
> Son inviolables los documentos privados y las comunicaciones escritas, orales o de cualquier otro tipo de los habitantes de la República. (Rivera, 2003: 16).

Interceptación de correo electrónico

Este problema es de especial importancia en el campo del comercio electrónico. La forma para contrarrestar el problema ha sido la encriptación de los mensajes por medio de la criptografía simétrica o asimétrica, e incluso el uso de la firma digital que permite verificar la procedencia, autenticación y la integridad del mensaje. Sin embargo, el problema del borrado de un mensaje no

se resuelve con la tecnología de encriptación y firma digital, se requiere de otros mecanismos adicionales para esto.

El artículo 196 bis del Código Penal regula la violación de comunicaciones electrónicas con pena de prisión de seis meses a dos años al que vulnere la intimidad de otro sin su consentimiento, apoderándose, accediendo, modificando, alterando, suprimiendo, interceptando, interfiriendo, utilizando, difundiendo o desviando de su destino mensajes, datos e imágenes contenidas en soportes electrónicos, informáticos, magnéticos y telemáticos.

El problema es determinar la identidad del infractor y su ubicación.

Por otro lado, no es delito que terceros tome las comunicaciones privadas de un usuario, si el usuario conscientemente accedió a un sitio y dio información personal, conociendo que el sitio o el mismo sitio le advirtió que no era seguro, y aún así lo hizo (artículo 26 de la Ley 4573 Código Penal).

Muchos servidores de correo electrónico dan un "login" y "password" de forma gratuita para tener una dirección de correo, y advierten que no son responsables por las violaciones a la intimidad que puedan sufrir en su servidor. Por lo tanto, de acuerdo con el artículo 26 del Código Penal (Ley 4573), si soy consciente de que mi intimidad no está resguardada en un servidor público y así lo manifiesto al suscribir los servicios gratuitos no sería delito el que otra persona tome mis comunicaciones de correo y los lea o los envíe a terceros.

Proxenetismo

Está regulado en el artículo 169 del Código Penal vigente y en el 170 en su figura agravada. Consiste en aquella actividad que persiguiendo un ánimo de lucro o la satisfacción de deseo ajenos, promueva o facilite la prostitución de personas de uno u otro sexo, y agravado en los casos en los que medie violencia, coerción, abuso de autoridad, si se trata de un menor de edad, o si el sujeto activo es el tutor, guardador o padre de la víctima.

En la Red, el proxenetismo ha encontrado una gama de posibilidades para desarrollarse al margen de la Ley, y Costa Rica no se encuentra alejada de esta realidad. Costa Rica es promocionada en muchas páginas de Internet como un "paraíso sexual", sin que se pueda llegar a configurarse una conducta delictiva, salvo en el caso de menores.

La debilidad de la regulación de este ilícito se encuentra en la competencia jurisdiccional para juzgar la responsabilidad del proxeneta que promueve por medio de la Red los servicios de sus víctimas. Si el proxeneta reside en el país, aunque la página se encuentre en un servidor extranjero puede ser procesado por la legislación costarricense.

El conflicto de competencia territorial inicia cuando el proxeneta se encuentra fuera del país en donde se ejecuta el hecho delictivo. Toda la labor de promoción, cobros, administración y concertación con cada cliente, y a la vez con sus víctimas, a través de la Red, sin tocar suelo costarricense.

El artículo 172 del Código Penal regula el delito de trata de personas, indicando que será sancionado con pena de prisión al que promueva, facilite o favorezca la entrada o salida del país de personas de cualquier sexo, para que ejerzan la prostitución o para mantenerlas en servidumbre sexual o laboral.

Sin embargo, otro problema es ubicar e identificar al infractor y aplicarle la Ley costarricense, y es posible que no se pueda extraditar, por lo que el delito queda impune.

Por otro lado, están los proveedores de servicios de Internet (PSI), que son dueños de los servidores en donde se instalan las páginas de promoción de una empresa. En este caso, de promoción de la prostitución. Sería proxeneta el dueño del servidor en el que se encuentre una página de esta naturaleza? El problema, con respecto a la responsabilidad de los PSI, ha sido discutido. Uno de los problemas que presenta el control de los PSI es la dificultad de vigilancia por la inmensa cantidad de información que se almacena de manera que se deja impune la conducta de los PSI.

Pornografía

Es difícil definir este concepto. Para algunos "pornografía" significa habilitar la libertad de expresión y un arte, para otros un mal que perturba la psique, así como la explotación y causa de desigualdades de género, por lo que cada ser humano tendrá su propia concepción sobre una fotografía de un desnudo en la red.

Son precisamente estas valoraciones subjetivas las que originan los diferentes argumentos sobre la necesidad o no de prohibir la pornografía en un territorio determinado, así como lo que se entenderá dentro de esa concepción.

Entre los argumentos en contra de la pornografía está el religioso, y desde el cristianismo, la sexualidad debe encaminarse a la procreación. El placer cuya única finalidad no sea la procreación sería pecaminoso.

> Para la feministas, la pornografía es una práctica discriminatoria basada en sexo que deniega a la mujer igualdad de oportunidades en la sociedad... La pornografía es una práctica sistemática de explotación y subordinación basada en la diferencia de sexos que daña a la mujer. (Salas y Sánchez, 1999: 162).

El Código Penal eleva esta figura al rango de delito, con la finalidad de proteger a los menores de edad. Los artículos 173 y 174 protegen a los menores de la pornografía, sin embargo, en la Red es muy fácil que los menores puedan tener acceso a este tipo de material. La mayoría de las páginas de este tipo tiene una advertencia para sus visitantes, de manera que no se trata de un acceso accidental. Existen "softwares" que introducen un nivel de regulación de la información a la que tiene acceso un computador específico y restringe algunas consultas. Esto permite que los padres de familia instalen este tipo de "softwares" para evitar que sus niños accedan a páginas con contenidos pornográficos.

La problemática se plantea principalmente sobre la pedofilia, pues existen muchos lugares en Internet dedicados a la explotación pornográfica de menores de edad.

El ordenamiento jurídico vigente no contiene normas que pueda enfrentar este problema. Aunque se tiene los artículos 173 y 174 del Código Penal, se presenta el problema de que no es un delito internacional (la pornografía pedófila) pues no es un problema de trata de blancas, y también cuando se trata de un sujeto que promueve la pornografía pedófila pero desde un país que no tenga prohibición alguna aunque se pueda castigar en Costa Rica, su actividad queda impune. El problema del principio de territorialidad y la falta de convenios internacionales

que regulen la novedosa criminalidad ponen obstáculos para la sanción de estas conductas.

Además, si el delincuente realiza las actividades a través de la red, es muy difícil su identificación y ubicación, y por tanto es difícil iniciar cualquier proceso penal al respecto.

Conclusiones y Recomendaciones

De acuerdo con el análisis presentado, los vacíos de la legislación existente se pueden resumir en las siguientes:

1- No existe jurisdicción que sea capaz de juzgar delitos transfronterizos o no son ágiles y eficaces. No es nada ágil ni eficaz iniciar un proceso judicial o administrativo contra una persona que ostenta una actividad ilícita que se encuentre en un servidor en el extranjero.
2- Los delitos de proxenitismo quedan impunes cuando el proxeneta se encuentra fuera del país, cuando toda la labor de promoción, cobros, administración y concertación con cada cliente, y a la vez con sus víctimas, a través de la Red, se realiza sin tocar suelo costarricense. El problema es ubicar al infractor y aplicarle la ley costarricense.
3- El ordenamiento jurídico vigente no contiene normas que pueda enfrentar el problema de la pornografía pedófila. Aunque se tiene los artículos 173 y 174 del Código Penal, se presenta el problema de que no es un delito internacional pues no es un problema de trata de blancas, y también cuando se trata de un sujeto que promueve la pornografía pedófila pero desde un país que no tenga prohibición alguna aunque se pueda castigar en Costa Rica. Su actividad queda impune. El problema del principio de territorialidad y la falta de convenios internacionales que regulen la novedosa criminalidad ponen obstáculos para la sanción de estas conductas.
4- La frase "o cualquier otra acción" del artículo 217 bis podría generar problema de inconstitucionalidad pues no individualiza las acciones penadas por ley requisito para la Ley Penal.
5- En cuanto al sabotaje en la red, el problema es que no hay norma que permita juzgar en el exterior, o podría ocurrir que no pueda llevarse a cabo la extradición, por lo que el delito quedaría impune. Es necesario que los delitos informáticos tenga elementos comunes entre los diversos países, de forma tal que pueda haber una sanción eficaz cuando se cometen desde fuera del país.
6- Acerca de las falsificaciones de datos, no hay una referencia clara en el Código Penal al documento electrónico que puede ser sujeto de falsificación o alteración. Es necesario una referencia explícita del término documento electrónico.
7- Se debe hacer los cambios legales para permitir insertar el documento electrónico como documento público. Aunque ya ha sido promulgada la Ley 8454 y su Reglamento, todavía no está implementado, pero ya es un gran avance.
8- Los accesos no autorizados a través de claves es un delito informático que debe ser contemplado, para ir protegiendo los sistemas que contienen

información secreta (bancos, tribunales, tributación, presidencia, etc.).

Los elementos principales para evitar la comisión de delitos están:

- Buenos mecanismos para la identificación de las partes.
- Seguridad para la información que viaja a través de la red. Para esto se han creado diferentes mecanismos e instrumentos destinados a proteger la información como las técnicas de encriptación, técnicas de identificación computarizada, certificados digitales, autoridades certificadotas, firma digital
- El uso murallas y claves de accesos.
- Utilización de software que filtran información no deseada.
- Utilización de licencias de programas, o registro de ellas.
- Implementar a nivel organizativo y administrativo, protocolos de actuación de seguridad, auditorías, y otros mecanismos en los centros de almacenamiento y procesamiento de datos para proteger los sistemas de información de accesos no autorizados, daños fortuitos y otros.

Lo más importante es la necesidad de un marco jurídico que haga posible la sanción al delito cibernético.

El Estado debe crear nuevos órganos con amplias facultades para conocer y perseguir a los delincuentes informáticos incluyendo a los que se encuentren en el extranjero.

Con la utilización de leyes modelo y entidades reguladoras creadas por organismos internacionales a los que los Estados se adhieren mediante tratados internacionales, se daría una uniformidad de criterios internacionales que asegurarían aunque sea de forma básica la protección de los ciudadanos en las actividades que se realizan en la Red.

La legislación costarricense ya incluye en varias de sus leyes el concepto de documento electrónico, también ha tipificado el delito informático para tres casos exclusivos: violación de comunicación, fraude y sabotaje informático. Sin embargo existen otros tipos de delitos informáticos que de alguna manera ya se contemplan en nuestra legislación pero que por la forma en que se dan quedan impunes, como por ejemplo, proxenetismo y pornografía.

Se requiere de un marco jurídico en el país que:

- Confiera seguridad jurídica y tecnológica a los usuarios de Internet
- Provea los mecanismos para identificar y sancionar a los infractores.
- Garantice un acceso ilimitado a toda la sociedad costarricense a este nueva forma de comunicación
- Sea abierta ante la posibilidad de las nuevas tecnologías.
- Refuerce los mecanismos de autorregulación y las leyes existentes.
- Confiera no solo la validez del documento electrónico y de la firma digital sino que regule, informe y eduque al ciudadano todo lo concerniente al Comercio Electrónico especialmente a la contratación electrónica.
- Garantice una justicia pronta y cumplida para los usuarios que se vean afectados por los delitos cometidos.

Es importante revisar esta materia a la luz de los estudios, análisis y acuerdos tomados por las principales organizaciones mundiales como: Organización

Mundial del Comercio (OMC), Organización para la Cooperación y Desarrollo del Comercio (OCDE por sus siglas en inglés), Conferencia Ministerial sobre Comercio Electrónico, Asociación Internacional Fiscal (International Fiscal Association, IFA), Unión Europea (UE), Área de Libre Comercio de las Américas (ALCA), MERCOSUR, Comunidad Andina de Naciones (CAN). Y estudiar las posibilidades de que el país se adhiera a estos convenios o acuerdos de grupo de países.

El Estado tiene el deber de encontrar los mecanismos válidos para que pueda tutelar los derechos de los ciudadanos, empresas y del propio Estado, los cuales se ven claramente en indefensión cuando se trata principalmente de transacciones internacionales electrónicas. Y conjuntamente realizar este control y vigilancia sin limitar las posibilidades de desarrollo de este tipo de tecnologías de información y comunicación.

Por último, es necesario realizar un estudio más amplio e integral sobre los delitos informáticos, que incluya además de los analizados, los relacionados con la propiedad intelectual, comercio electrónico, hacienda, protección a la privacidad e intimidad, y protección al consumidor, entre otros; y que se realice las inclusiones o modificaciones necesarias a las leyes y proyectos de leyes respectivas.

Referencias bibliográficas

Asamblea Legislativa**.** (1999). *Ley 4573. Código Penal, con reformas de la Ley 7899 del 3 de agosto de 1999.* Costa Rica. Consultado el 20 enero de 2007 en http://www.secmca.org/archivos/Codigo%20Penal.pdf.

Asamblea Legislativa. (1971). *Ley 4755 Código de Normas y Procedimientos Tributarios.* Costa Rica. Consultado el 1 de febrero de 2007 en http://www.racsa.co.cr/asamblea/ley/leyes/6000/4755.doc .

Asamblea Legislativa. (1989). *Ley 7130. Código Procesal Civil.* Costa Rica: Sistema Costarricense de Información Jurídica. Consultado el 21 de enero de 2007 en http://www.pgr.go.cr/scij/index_pgr.asp?url=busqueda/normativa/normas/nrm_articulo.asp?nBaseDato=1&nNorma=12443&nVersion=6&nArticulo=71404.

Asamblea Legislativa.(1990). *Ley No.7202. Ley Sistema Nacional de Archivos.* Costa Rica. Consultado el 21 de enero de 2007 en http://www.tse.go.cr/Ley_arch.htm.

Asamblea Legislativa.(1994). *Ley No. 7425. Ley de Registro, Secuestro y Examen de documentos privados e intervención de las comunicaciones.* Costa Rica. http://www.racsa.co.cr/asamblea/ley/leyes/7000/7425.doc 15-1-07

Asamblea Legislativa. (1995-a). *Ley No.7494. Ley de Contratación Administrativa.* Costa Rica. Consultado el 21 de enero de 2007 en http://www.asamblea.go.cr/ley/leyes_numero.htm

Asamblea Legislativa. (1995-b). *Ley 7535 de Justicia Tributaria.* Costa Rica. Consultado el 22 de enero de 2007 en http://www.racsa.co.cr/asamblea/ley/leyes/7000/7535.doc

Asamblea Legislativa. (2001-a). *Ley 8131 de Administración Financiera de la República y Presupuestos Públicos.* Consultado el 13 de abril de 2007 en http://www.asamblea.go.cr/ley/leyes_nombre.htm

Asamblea Legislativa. (2001-b). Ley 8148 adición de los artículos 196 bis, 217 bis y 229 bis al código penal ley Nº 4573, para reprimir y sancionar los delitos informáticos. Costa Rica. Consultado el 22 de enero de 2007 en http://www.racsa.co.cr/asamblea/ley/leyes/8000/8148.doc

Asamblea Legislativa. (2002). Ley 8238 reforma de la ley de registro, secuestro y examen de documentos privados e intervención de las comunicaciones, Nº 7425, de 9 de agosto de 1994, y sus reformas. Costa Rica. Consultado

el 17 de enero de 2007 en http://www.racsa.co.cr/asamblea/ley/leyes/8000/8238.doc

Asamblea Legislativa. (1993). *Ley 7333 Orgánica del Poder Judicial*. Costa Rica. Consultado el 20 enero de 2007 en http://www.asamblea.go.cr/ley/leyes_numero.htm

Asamblea Legislativa. (1995-c). *Ley No.7494. Ley de Contratación Administrativa*. Costa Rica. Consultado el 21 de enero de 2007 en http://www.asamblea.go.cr/ley/leyes_numero.htm

Asamblea Legislativa. (1995-d). *Ley No.7557. Ley General de Aduanas*. Costa Rica. Consultado el 3 de abril de 2007 en http://www.racsa.co.cr/asamblea/ley/leyes/7000/7557.doc

Asamblea Legislativa. (2005). *Ley 8454 de Certificados, Firmas Digitales y Documentos Electrónicos, publicada 30-08-05*. Costa Rica: Sistema Costarricense de Información Jurídica. Consultado el 15 de enero de 2007 en http://www.pgr.go.cr/

Asamblea Legislativa. (2003). *Proyecto de Ley 15178 de Protección de la Persona frente al Tratamiento de sus Datos Personales*. 27 de marzo 2003. Costa Rica. Consultado 3 abril de 2007 en http://www.racsa.co.cr/asamblea/proyecto/buscar/exped12.htm

Carvajal, T., Jiménez, S. (2002). *Cláusulas abusivas en contratos de adhesión en Internet*. Tesis para optar por el grado de Licenciatura en Derecho. Facultad de Derecho. Universidad de Costa Rica.

Chinchilla, C. (2002). *Delitos Informáticos*. 1a ed. San José: IJSA.

Echegaray, E. (2001). *Comercio electrónico y una necesaria regulación para la protección de los derechos del consumidor*. Tesis de grado para optar por el título de Licenciatura en Derecho. Facultad de Derecho. Universidad de Costa Rica.

Herrera, R. (1999). El documento electrónico: algunas vías de aplicación en el derecho probatorio chileno. *Revista Electrónica de Derecho Informática.(REDI)*. No.7. febrero 1999. Consultado el 20-01-07 en http://www.alfa-redi.org/rdi-articulo.shtml?x=225

Lewis, E. (2006). *Delitos Informáticos de Costa Rica 2004-2005*. San José: Datos de Expedientes en Archivos del Organismo de Investigación Judicial. Sección de Delitos Informáticos.

Monge, B., Murillo, T. (2000). *La seguridad jurídica de la compraventa mercantil por medio de Internet*. Tesis para optar por el grado de Licenciatura en Derecho. Facultad de Derecho. Universidad de Costa Rica. Costa Rica.

Ramos, F. (1998). Problemas jurídicos del comercio electrónico. *Revista Electrónica de Derecho Informático*. 2-Set-1998. Consultado el 15 de enero de 2007 en http://publicaciones.derecho.org/redi/N@mero_10_-_Mayo_de_1999/ramos2.

Rivera, G. (2003). Constitución Política de la República de Costa Rica. San José: Editec Editores S.A.

Salas, J., Sánchez, J. (1999). *Algunas figuras delictivas en Internet*. Tesis para optar por el grado de Licenciatura en Derecho. Facultad de Derecho. Universidad de Costa Rica. Costa Rica.

Solano, Monserrat. (2001). Atención a ciberdelitos. La Nación. 1 de junio de 2001. San José, Costa Rica. Consultado el 28 de febrero de 2006 en http://www.nacion.com/ln_ee/2001/junio/01/pais15.html

Téramond, C., Fernández, M. (2002). *Concepto, valor jurídico y regulación de la firma digital en Costa Rica*. Tesis para optar por el grado de Licenciatura en Derecho. Facultad de Derecho. Universidad de Costa Rica. Costa Rica.

Téllez, J. (2004). *Derecho Informático*. 3 ed. México: McGraw Hill/Interamericana Editores S.A.