Universidad Latinoamericana de Ciencia y Tecnología (ULACIT)

Facultad de Ingeniería

Escuela de Ingeniería Informática

"Atipicidad relativa en los delitos informáticos en el código penal de Costa Rica"

Autor: Iván Rojas Álvarez[1]

Profesor: Miguel Pérez Montero

San José, Costa Rica
2005

[1] Bachiller en Informática. Candidato a Licenciatura en Informática con énfasis en Telemática y Redes, ULACIT. Correo electrónico: ivanr@costarricense.cr

DEDICATORIA

Quisiera dar gracias a DIOS por permitirme transitar este camino y por ponerme a personas tan maravillosas a mí alrededor.

Este trabajo esta dedicado a mi esposa e hija que son la luz que iluminan mi día, que cada vez que pienso en ellas me dan fuerzas para seguir adelante en busca de un mejor futuro.

Además quiero dedicar este trabajo a mi madre, mi papá y mi hermana por el apoyo incondicional que me han ofrecido a lo largo de mi vida, sin el empuje que me han brindado sería muy difícil haber llegado hasta donde estoy el día de hoy.

Resumen

El cambio tecnológico que se ha vivido desde mediados de siglo ha producido efectos en todas las áreas del quehacer humano. Cuando se habla de tecnología, no puede dejarse de hacer alusión a la informática y a las telecomunicaciones. Estos dos fenómenos han hecho que la humanidad entrara en la era de la información. Atrás ha quedado la etapa agrícola y la etapa industrial.

Este cambio abrupto que ha tenido la humanidad gracias al Internet produjo que así como se incrementaba su uso, también se incrementaran los llamados delitos informáticos. Muchos de estos delitos se dan gracias a la extraterritorialidad, la dificultada para la investigación, la disociación temporal, etc.

La cifra alarmante de la criminalidad, en materia de delitos informáticos, no puede seguir en aumento, de allí la necesidad imperiosa para el derecho penal y organismos gubernamentales de la investigación de una modalidad de amplias repercusiones sociales y económicas. Existe una necesidad urgente de incluir o modificar en el derecho penal vigente una tipificación básica de los delitos informáticos que afecten el interés social y el patrimonio público.

Abstract

The technological changes experienced since the mid-twentieth century have affected all human beings' tasks. When speaking of technology, it is impossible not to make allusion to computer science and telecommunications. These two phenomena have placed humankind at the doorsill of the information era; the agricultural and industrial epochs have been left behind.

Thanks to Internet, humanity has had an abrupt change; which at the same time has also provoked an increment in its use as well as increment in the so-called: computer crime. Many of these crimes take place due to the extraterritoriality, the difficulty to investigate, the temporal disassociation, etc.

This alarming level of criminality (in terms of computer crime) must not continue to increase. Therefore, it is necessary for the criminal law and mandatory for some governmental organizations to initiate a broad investigation with social and economical repercussions. The actual Criminal Code urges an inclusion or modification of a basic typification of the computer crimes that affect the public interest and our patrimony.

Palabras claves

Delito informático / código penal / ética informática / antecedentes legislativos / jurisprudencia.

“Atipicidad relativa en los delitos informáticos en el código penal de Costa Rica”

La cifra alarmante de la criminalidad, en materia de delitos informáticos, no puede seguir en aumento, de allí la necesidad imperiosa para el derecho penal y organismos gubernamentales de la investigación de una modalidad de amplias repercusiones sociales y económicas. Existe una necesidad urgente de incluir o modificar en el derecho penal vigente una tipificación básica de los delitos informáticos que afecten el interés social y el patrimonio público.

Actualmente se requieren serias modificaciones y en otros casos nuevas normas para disminuir en cierta forma la incertidumbre jurídica en que se encuentran sumergidas las nuevas disposiciones penales en materia de delito informático, pese a algunos avances, como la ley número 8148 emitida durante el gobierno del señor Miguel Ángel Rodríguez Echeverría.

Cada vez más, se hace necesario el respaldo legal como la mejor y más adecuada forma de reprimir y castigar estos delitos, tal como se expondrá más adelante en la conveniencia de su incriminación y el sistema más adecuado para Costa Rica, según su tradición jurídico-legal. Las conductas reprochables, resultan en la mayoría de los casos impunes debido a la falta de las figuras incriminatorias tradicionales, al no ser castigados dichos comportamientos ilícitos, debido a la carencia de claridad sobre la naturaleza jurídica de los bienes objeto material de los delitos.

También se expondrán en este artículo cada una de las modificaciones a las conductas punibles contra el patrimonio ajeno, que necesitan de verdaderos cambios, con miras de que exista en este país una penalización de la criminalidad informática. Al igual se darán las conclusiones donde se expondrán ideas, sobre la forma como enfrentar esta problemática social. Es oportuno aclarar, que este artículo se circunscribe únicamente a delitos contra el patrimonio ajeno y se hará mención de otras conductas que lesionan otros bienes jurídicos.

El estado actual de adecuación normativa está en una categoría sui géneris, ya que dichas infracciones no se adaptan en las actuales formas descriptivas, pese a que ya las contienen la mayoría de legislaciones penales.

Crear o modificar es el dilema, decidir si conviene crear una ley individual sobre la materia o si los diversos tipos penales deben ser encasillados en diferentes capítulos del Código Penal costarricense.

Definición de los delitos informáticos a nivel mundial

Para *Irving J. Sloan* hablar de delito informático no implica sólo un delito cometido por medio de computadores. Según el citado autor un delito informático consiste "en el uso de una computadora como instrumento de un delito económico" (1984,2). Continua Sloan explicando que los computadores pueden tener varios roles en el delito. Estos son como

- Objeto
- Sujeto
- Instrumento
- Símbolo

Para otro autor como *Correa* delito informático es "cualquier conducta ilegal, no ético, o no autorizada que involucra el procesamiento automático de datos y/o la transmisión de datos" (1987,295)

Resulta difícil llegar a un consenso en lo que al delito informático se refiere, pero después de revisar diversas definiciones se podrá llegar a la conclusión de que es el acto en el cual interviene un sistema de cómputo como objeto o sujeto en la producción de un hecho criminológico, en donde se atenta contra los derechos y libertades de los ciudadanos.

A continuación se citan y definen algunos de los delitos informáticos más comunes hoy en día, como se hará ver más adelante el crimen informático es cambiante en el tiempo, por lo que sería casi imposible hablar de todos ellos.

Intrusismo informático:

Se entiende por intrusismo informático la entrada en un sistema o en un ordenador sin consentimiento, como una especie de allanamiento de morada. El denominado "hacking blanco", se da simplemente por curiosidad o placer y de reto constante a modo de desafío intelectual del intruso para descubrir la vulnerabilidad del sistema, pero sin intentar explotar en beneficio propio los puntos débiles del sistema.

Espionaje informático:

Se debe de entender por la obtención, sin autorización, de datos almacenados en un fichero informático; violando así secretos o la intimidad.

Sabotaje informático:

Se trata de interferencias en el funcionamiento adecuado del sistema, mediante la inserción, transmisión, alteración, daño o supresión de datos informáticos. Dicho daño puede darse tanto en la parte física del ordenador (hardware) como a la parte lógica del mismo (software)

Uso indebido de instalaciones y/o abuso de equipos:

Puede ser el caso de empleados desleales que utilizan las instalaciones para su propio beneficio, o para perpetrar alguna conducta ilícita. Además de la fabricación, distribución y venta de equipos de acceso diseñados para abusar de las redes o de los sistemas informáticos.

Fraude informático:

Llevar a cabo manipulaciones con la intención de que tenga lugar una transferencia ilegítima de propiedad en perjuicio de tercero, el legítimo propietario. Por ejemplo con las tarjetas de crédito, compras fraudulentas a través de Internet, etc.

Alteración de bases de datos:

Las bases de datos se han convertido en la estructura vertebral de Internet, sin perjuicio de la importancia de los protocolos y de las aplicaciones que están a la vista del ínter nauta y cuya importancia consiste en hacer visualmente más agradable la información. Las bases de datos se utilizan para almacenar cualquier tipo de información en sentido amplio, por lo que cualquier cambio puede afectar significativamente.

Internet, propiedad intelectual y derechos conexos:

La ilimitada posibilidad de replicación es una de las características orgánicas de la informática y con la difusión de las redes, se favoreció tanto la copia desde lugares distantes como la transmisión de lo ya copiado.

La copia no autorizada de programas de computador o de música, libros; es una clara violación a los derechos de propiedad intelectual que existen en cada uno de ellos.

El enmascaramiento:

El enmascaramiento supone fingir que se es un computador diferente al que se está utilizando; consiste por consiguiente en enviar al ordenador destino una serie de data gramas con una cabecera falsa en la que se ha alterado la identificación del remitente.

Basados en los anteriores tipos de delitos informáticos se pueden dividir en cinco grandes grupos para un mayor entendimiento, los cuales son:

- Delitos contra el patrimonio: La mayoría de los delitos cometidos por medios de computadores tiene relación con el patrimonio, esto se debe en gran medida a la delegación a máquinas de las tareas cotidianas, pero también por la transformación del dinero tradicional a nuevas formas como dinero plástico y dinero electrónico.
- Delitos contra la intimidad: Como se ve en la actualidad la información ha tomado un valor preponderante, ya que se le trata como una mercancía; ello produce que se comercie con datos de carácter personal, a veces invadiendo de este modo la intimidad personal.
- Delitos contra la seguridad pública y las comunicaciones: La informática está inmersa en nuestras vidas y cada día somos más dependientes de ella y su funcionamiento para realizar cualquier tarea. Por lo anterior es que se dan ataques que superan lo individual para pasar a lo colectivo afectando así la seguridad pública.

- Falsificaciones informáticas: La falsedades cometidas por medios informáticos se constituyen en un delito, porque en general los documentos electrónicos han adquirido un valor jurídico muy importante y en caso de no ser así , se usa como elemento para tomar decisiones, a veces automáticamente y otras no.
- Contenidos ilegales en Internet: La evolución que tuvo y que tiene Internet la hace que sea invadida por una gran cantidad de material ilícito, como propaganda discriminatoria o con contenidos pornográficos y pedófilos.

Polémica por la existencia de los delitos informáticos

El cambio tecnológico que se ha vivido desde mediados de siglo ha producido efectos en todas las áreas del quehacer humano. Cuando se habla de tecnología, no puede dejarse de hacer alusión a la informática y a las telecomunicaciones. Estos dos fenómenos han hecho que la humanidad entrara en la era de la información. Atrás ha quedado la etapa agrícola y la etapa industrial. El advenimiento de las telecomunicaciones y su fusión con la informática ha llevado a algunos autores a afirmar que estamos en la era digital.

Este cambio abrupto que ha tenido la humanidad gracias al Internet produjo que así como se incrementaba su uso, también se incrementaran los llamados delitos informáticos. Muchos de estos delitos se dan gracias a la extraterritorialidad, la dificultada para la investigación, la disociación temporal, etc.

A continuación se desarrollan los aspectos antes mencionados que ayudan a la criminalidad informática, al mencionar a la dificultad para la investigación se ve el hecho de que el delito informático es más difícil de investigar que el delito tradicional, esto por cuanto es un tanto novedoso, escapa a los cánones tradicionales y los cuerpos policiales y tribunalicios no están preparados para investigar y detectar estas técnicas o no cuentan con las herramientas necesarias para llevar acabo dicha investigación.

Otro aspecto que colabora con los delitos es la extraterritorialidad ya que en la parte criminológica el factor espacio y tiempo constituyen elementos de riesgo que el delincuente no tendrá que tomar en cuenta al momento de cometer la acción ilícita; ya que en los delitos informáticos estos dos factores se ven altamente disminuidos.

La disociación temporal presenta otro aspecto a tomar en cuenta ya que existe la posibilidad de programar la ejecución de un delito informático en una determinada fecha, por lo que la disociación no es entonces sólo espacial sino también temporal. Dicha programación no esta estrictamente ligada con la comisión del delito, sino que puede constituir una forma de obstruir la investigación del mismo, esto por cuanto se puede llegar a programar que al detectar un acceso eliminen cierta información o que avisen al propio autor del delito que puede estar siendo investigado. (Corea, 1987,295)

Vale la pena hacer una reseña de los daños ocasionados por la criminalidad informática. En todos los estudios, informes y estadísticas se encuentran dos temas comunes: montos sumamente considerables y que cada año los delitos por computadora se incrementan.

En los últimos años se ha notado un aumento de la criminalidad relacionada con computadoras. En parte ello se debe al gran desarrollo que la informática y la telemática han experimentado, haciendo cada vez más común el uso de las computadoras en las tareas más cotidianas.

El incremento de la criminalidad informática tiene su origen en diversos factores. Un estudio realizado en Europa detectó las siguientes causas:

- Descentralización de sistemas, que hace que el usuario tenga un rol más importante y mayor acceso a los recursos del sistema informático.
- Conexión de sistemas informáticos entre sí. Esto tiene lugar dentro de una misma empresa, entre distintas empresas y tanto a nivel nacional como internacional. El ejemplo clásico es Internet.
- A los anteriores se agrega el incesante desarrollo del dinero electrónico, que permite su transferencia y manejo sin su necesaria traslación física.

Es importante resaltar el hecho que muchos de los delitos informáticos que se comente a través del mundo entero se siguen dando debido a la falta de denuncias por parte de las compañías afectadas, esto por cuanto muchas veces prefieren guardar silencio, antes que dar a conocer sus fallas de seguridad ante los clientes, perdiendo así la confianza depositada en ellos. En un porcentaje menor no se da la denuncia muchas veces por que consideran que no tendrán respaldo o sustento legal para llegar hasta las últimas consecuencias, en busca de normativas que repriman el delito.

Para finalizar, hay que resaltar que los diferentes delitos informáticos cometidos hoy en día no miran si afectan a una empresa privada, al sector gobierno o a un solo individuo, o el país donde se comete el hecho; lo único que les interesa a sus victimarios es conseguir su acto vandálico provocando así en su víctima un alto perjuicio económico, así como en muchos ocasiones problemas que van más allá del factor económico.

Antecedentes legislativos del delito informático en otros países:

La evolución tecnológica ha generado un importante número de conductas nocivas que, aprovechando el poder de la información, buscan lucros ilegítimos y causan daños. El derecho que por esencia se muestra reticente al cambio, no ha reaccionado adecuadamente a las nuevas circunstancias. La importancia de la información se encuentra presente en todos los ámbitos de la vida del ser humano. La informática puede ser el mejor aliado o el peor enemigo del hombre, dependiendo del uso que éste le dé.

Así como el desarrollo informático ha proporcionado al hombre beneficios importantes, de igual manera ha dado lugar a ciertas conductas ilícitas. La sociedad informatizada es tecnológicamente vulnerable y el avance tecnológico no ha sido acompañado de la creación de defensas en el campo jurídico. De este modo el derecho penal está siendo desbordado por la aparición de delitos que en otra época jamás se imaginaron.

Es así como ante este nuevo reto los sistemas jurídicos de algunos países se han modificado para dar la cabida a nuevas normas jurídicas que ayuden a prevenir las conductas ilícitas provenientes de la utilización de medios informáticos.

España

España es uno de los países que mayor preocupación ha mostrado sobre el tema, muestra de ello es que ha introducido o más bien ha tenido un acercamiento con los ya denominados delitos informáticos por medio de una gran cantidad de leyes creadas en muy corto tiempo. Ejemplo de esto es el Código Penal y otras leyes especiales como la LORTAD (ley Orgánica de Regulación del Tratamiento Automatizado de Datos).

Durante la primera mitad de 1996 entra en vigor la ley orgánica del código penal, la cual busca regular en forma específica las nuevas formas de delincuencia ya que con el anterior texto penal se estaba incurriendo en la atipicidad, problema que la jurisprudencia española había estado solucionando de forma artificiosa. El fin de la nueva ley era introducir nuevas figuras delictivas para responder a las necesidades de la sociedad actual.

La nueva ley provee regular aquellas acciones delictivas que no tenían sanción hasta la fecha, las agrupan en:

Delitos contra la intimidad y el derecho de la propia imagen: se busca proteger los diversos documentos que contengan secretos de una persona y dentro de los cuales están los mensajes de correo electrónico, haciendo de esta forma una referencia clara a la informática.

Delitos contra el patrimonio y contra el orden socioeconómico: es interesante la posición que toma la legislación española con relación a los términos hurto y robo; ya que aclara en su nueva legislación que no es necesario que exista posesión material sobre el bien, ya que en los delitos informáticos no siempre existen; además si se habla de un programa computacional no se puede tomar ni es una cosa o mueble, como hablaba la legislación anterior.

Con esta regulación penal hecha en España se cubren una serie de lagunas de las cuales aquejaban dicho sistema. Otro aspecto a resaltar es el hecho de introducir el elemento informático en las injurias y calumnias ya que por medio de Internet bien pueden cometerse este tipo de delitos y además se pena al creador del software que se utiliza para la comisión de cualquiera de los delitos, equiparando la pena con la del autor del mismo.

Estados Unidos

Este país trata de estar a la vanguardia en cuanto a la sanción en contra de los delitos informáticos desde hace mucho tiempo, ejemplo de esto es el Acta Federal de Abuso Computacional de 1944 y la cual sufre modificaciones por el Acta de Fraude y Abuso Computacional de 1986.

Este país se enfoca principalmente a todo lo relacionado con los virus, gusanos y caballos de troya que afectan la informática moderna. Según sus legisladores la nueva ley constituye un acercamiento más responsable al creciente problema de los virus informáticos, específicamente no definiendo a los virus sino describiendo el acto para dar cabida en un futuro a la nueva era de ataques tecnológicos a los sistemas informáticos en cualquier forma en que estos se lleguen a realizar.

El objetivo que se perseguía con esta legislación, era aumentar la protección a los individuos, negocios y agencias gubernamentales de la interferencia, daño y acceso no autorizado a las bases de datos y sistemas computarizados creados legalmente. Es importante mencionar que en uno de los apartados de esta ley, se contempla la regulación de los virus conceptualizándolos aunque no los limita a un grupo de instrucciones designadas a contaminar a otros grupos de programas o bases de datos, modificar, destruir, copiar o transmitir datos o alterar la operación normal de las computadoras.

México

Aunque muchos han sido los esfuerzos en este país por regular este tipo de delitos y existen grandes expositores en esta materia, sobre la necesidad de normar la criminalidad informática, lo cierto es que no se encuentra mucha legislación con relación a este tema en el ordenamiento jurídico mexicano.

Las lagunas del derecho en este ordenamiento se hacen más evidentes cuando se analiza la normativa existente hasta este momento y se enfrentan a las nuevas modalidades informáticas. El código penal mexicano presenta serios problemas principalmente en tres artículos, los cuales son: el hurto, la estafa y el daño.

Se maneja una propuesta presentada por Pacheco Klein y en términos generales dicho proyecto realmente logra subsanar en gran medida la carencia normativa con relación a los delitos informáticos en el ordenamiento jurídico mexicano, ya que abarca figuras de muy variada naturaleza, es así como contempla los daños informáticos, el hurto informático, el fraude informático, etc; figuras que en la actualidad están en el código penal, pero que no comprende el elemento informático. Lamentablemente esta propuesta aún no ha sido implementada. (2001,150)

Pero pese a que en México la regulación específica en esta materia es sumamente escasa, esto no quiere decir que no existan normas referidas a este tema y que abarquen el tratamiento de datos informatizados; es así como en marzo de 1997 entra en vigor la ley

federal del Derecho de Autor; dicha ley regula todo lo referente a los programas de computación, las bases de datos y las infracciones derivadas de su uso

Ética Informática

La definición más restrictiva de la ética informática según JOHNSON es considerarla como la disciplina que analiza problemas éticos que son creados por la tecnología de los ordenadores o también los que son agravados por la misma, es decir, por las personas que utilizan los avances de las tecnologías de la información. (1996, 24)

Independientemente de la definición que se busque la tarea de la ética informática es aportar guías de actuación cuando no hay reglamentación o cuando la existente es obsoleta. Al vacío existente de políticas se debe añadir generalmente un problema de vacío conceptual. Por ello la ética informática también ha de analizar los dilemas éticos que ocasiona la informática.

La intención de la ética informática es incorporar una conciencia social relacionada con la tecnología informática y también ayudar a los informáticos a utilizar los computadores no solo con eficiencia sino con criterios éticos. El objetivo es tomar decisiones sobre temas tecnológicos de manera que se actué según los propios valores que uno profesa o con los de los derechos humanos en general.

Para ello esta disciplina se puede ver de varios objetivos; por un lado, descubrir y articular dilemas éticos clave en informática, determinar en qué medida son agravados, transformados o creados por la tecnología informática y ante los dilemas éticos que ocasiona la informática, analizar y proponer un marco conceptual adecuado para determinar qué hacer en las nuevas actividades ocasionadas por la informática en las que no se perciben con claridad las líneas de actuación a seguir.

La ética informática pretende tener en cuenta dos aspectos. Utilizar la teoría para clarificar los dilemas de esta índole y detectar errores en el razonamiento de la misma. Por otro, colaborar con otras disciplinas, siendo conscientes de los puntos de vista alternativos en las cuestiones referentes a valores y sabiendo discriminar entre las consideraciones éticas y las técnicas.

Las asociaciones de profesionales de informática y algunas empresas relacionadas con la informática han desarrollado códigos de conducta profesional. Estos códigos tienen distintas funciones, entre ellas:

- Que existan normas éticas para una profesión quiere decir que un profesional, en este caso un técnico, no es solo responsable de los aspectos técnicos del producto, sino también de las consecuencias económicas, sociológicas y culturales del mismo.
- Estas normas tienen una función sociológica ya que dan una identidad a los informáticos como grupo que piensa de una determinada manera; es símbolo de sus estatus profesional y parte de su definición como profesionales.

- Estas normas sirven también como fuente de evaluación pública de una profesión y son una llamada a la responsabilidad que permiten que la sociedad sepa qué pasa en esa profesión; aumenta la reputación del profesional y la confianza del público. (CPIC, 2004)

Sin embargo, la crítica que se hace a estas asociaciones es que han hecho poco por hacerlos cumplir, por imponer sanciones si no se cumplen o por comprobar si se aplican o si son relevantes o pertinentes. De hecho hay códigos que no son conocidos por los miembros de sus profesiones y menos por sus clientes. En general, también suelen faltar las medidas disciplinares, necesarias cuando las actividades de un miembro están en conflicto con la expresado dentro del código. También se critica que muchos códigos son el fruto del pensamiento tecnológico de los países desarrollados que no tienen en cuenta diferencias en valores sociales y culturales.

El que las asociaciones de profesionales de informáticos busquen códigos de ética que les obliguen a un modo de actuar tiene algo de positivo. Quiere decir que en esta sociedad tecnócrata los miembros de éstas se están haciendo conscientes de las consecuencias de su trabajo. Son los informáticos los que conocen en profundidad la naturaleza de los sistemas informáticos, la verdad sobre los sistemas de seguridad, los posibles daños por un mal uso del sistema y la verdadera intención de sus usuarios.

Los códigos son un paso en la toma de conciencia de las sociedades y organizaciones que quieren mejorar situaciones en las que los impactos sociales del desarrollo tecnológico no

se tienen en cuenta. “Cabe aclarar que lo que se dicta en los códigos no tienen que duplicar lo que existe en la ley; ya que la ley trata de la legalidad de las prácticas sociales, es normativa por definición y se impone con sanciones. Los códigos, en cambio, tratan del comportamiento según principios éticos, su normatividad no es más que mostrar una declaración de intenciones sobre la misión de una institución y en la mayoría de los casos la pena real con que se imponen es pequeña”. (JOHNSON, 1996, 41)

Se puede concluir que se está antes nuevos retos en el mundo profesional, los códigos de ética informática de lo s colegios o instituciones pretenden responder a las cuestiones éticas que surgen en la vida profesional. Sin embargo, no son una respuesta suficiente a los problemas derivados de la tecnificación de las profesiones, aunque sí un medio de plantearse los problemas y concienciarse de la relevancia de los mismos. Por otro lado, la ética informática supone un reto para la vida educativa, en el sentido de que educar en conciencia ética ha de ser también parte del currículo de los centros de enseñanza e investigación informática.

Necesidad sobre la penalización de la criminalidad informática

Es claro que es necesario que exista una penalización en cuanto a la criminalidad informática, pero primero se deberá ver como se puede realizar el cambio en el código penal existente, ya que es muy fácil decir sí a la penalización de dichos delitos pero el como se puede hacer es la parte más importante y delicada.

Existen varias formas hoy en día para actualizar el sistema penal, mediante cualquiera de ellas se podrán regular las conductas de delincuencia informática con las que se viven actualmente.

La primera de ellas es en la que se mira a la delincuencia informática como una tendencia muy próxima a las ya tradicionales conductas criminales previamente conocidas y reguladas por nuestro código penal; entonces se optará por reformar o agregar secciones o incisos a las figuras penales preexistentes para contemplar las nuevas modalidades tecnológicas de su ejecución. Dicha conducta hoy en día es la más práctica pero talvez no sea la más adecuada.

La otra alternativa es la que considera delincuencia informática como una clase de conducta criminal, de carácter unitario, se procurará normarlo mediante el diseño de un delito nuevo que se adicionará al respectivo código penal.

Dentro de las anteriores propuestas se puede ver que la última es tal vez la más perjudicial para un sistema, ya que resulta difícil alcanzar una redacción tan comprensiva y general que cubra con efectividad todas aquellas circunstancias en que la informática puede intervenir en la configuración de un delito. En la actualidad los proyectos de ley van orientados hacia la primera opción y se pretende realizar reformas parciales a delitos específicos, aprovechando así la nueva numeración e integrando la reforma al código penal en general.

De existir una fórmula única y más eficiente sería buscando un punto intermedio en donde se considere a la delincuencia informática no solo como una manifestación novedosa sino, además como una que presenta múltiples facetas y vías de ejecución, probablemente se elegiría agregar un capítulo separado sobre delincuencia informática a nuestro código penal o a las respectivas leyes especiales que lo pretendan regular.

Se habla también de las leyes o convenios entre diferentes países como es el caso del Consejo de Europa para la armonización de los delitos informáticos; en dicho convenio se prevé establecer cooperación internacional para la prevención y persecución de los delitos cometidos mediante o a través de ordenadores y, por otro lado, establece un mandato a las partes signatarias para desarrollar una legislación nacional coherente entre ellos y represiva de los delitos informáticos.

Un aspecto a resaltar de los convenios como el citado anteriormente es que pretende eliminar la diferencia que existe entre países en cuanto a la penalización de los delitos informáticos, ya que no permite que una misma conducta, en la cual la lesión al bien jurídico resulta de la misma gravedad, se regule en diferentes países con penalidades distintas. Un ejemplo claro de esto y se aplica solo en nuestro país, tan siquiera es con relación a otros países es "las diferencias que existentes entre la Ley General de Aduanas, Ley de Administración Financiera de la República y Presupuestos Públicos y la Ley Tributaria, por cuanto al supuesto de apoderarse, copiar, destruir, inutilizar…sin la autorización de la administración, programas de computación o bases de datos de uso

restringido se penaliza en unos con prisión de uno a tres años, mientras que en la otra ley se sanciona con prisión de tres a diez años". (Chinchilla,2002,93)

La conclusión a la que se puede llegar es que en nuestro territorio es más importante una ley que otra; esto no parece ser más que resultado de la improvisación legislativa, sin mediar conciencia de las normativas que se crean y las sanciones que se imponen. Las penas deben justificarse conforme el principio de daño causado, el cual permite determinar los tiempos mínimos y máximos de prisión.

Este tipo de problemas seguirán existiendo, en tanto no se procure la unificación de las regulaciones legales sobre la delincuencia informática.

Actualidad legal y jurisprudencia en materia de derecho informático en Costa Rica

Nuestro código penal de 1971 permaneció inalterado en su inclusión de ilícitos informáticos, desde su entrada en vigencia hasta la promulgación de la ley Nº 8184 del 24 de octubre del 2001, publicada en el diario oficial la gaceta del 21 de noviembre del mismo año. Con esta reforma se incorporaron tres disposiciones legales novedosas y de gran utilidad en la penalización y combate de la criminalidad informática. Sin embargo, la reforma fue escasa y se dejaron fuera muchos delitos de especial relevancia.

A continuación se señalaran algunos aspectos que abarcaron esta reforma:

Violación de comunicaciones electrónicas (artículo 196 bis)

Esta norma regula la violación de comunicaciones electrónicas en la cual el delito es comprendido de forma debida: "Será reprimida con pena de prisión de seis meses a dos años, la persona que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere, acceda, modifique, altere, suprima, intercepte, interfiera, utilice, difunda o desvíe de su destino, mensajes, datos e imágenes contenidas en soportes: electrónicos, informáticos, magnéticos y telemáticos". La pena será de uno a tres años de prisión, si las acciones descritas en el párrafo anterior, son realizadas por personas encargadas de los soportes: electrónicos, informáticos, magnéticos y telemáticos. (código penal, 1971)

Fraude informático (artículo 217 bis)

Este es tal vez la reforma más relevante en materia de criminalidad informática: "Se impondrá 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". (código penal, 1971)

Al oír el nombre que tiene este artículo lo primero que se piensa es relacionar fraude a un modus operandi, que caracteriza un determinado comportamiento, dirigido a una artimaña, que provoca determinada modalidad de acción. Por eso sería más claro asociarlo con la

definición de defraudación que se refiere al perjuicio económico ocasionado mediante el fraude.

Este segundo término refleja más adecuadamente la intención del artículo 217 bis; ya que no se habla de cualquier tipo de acción fraudulenta que surge con la utilización de medios informáticos, sino únicamente cuando lo dirigimos por la definición de defraudación. Muestra de ello es que no toda acción fraudulenta representa un perjuicio económico, puede caer en el campo del sabotaje informático.

Otro aspecto de dicho artículo es la palabra influir que no es muy clara en cuanto a su concepto, y le otorga la libertad de decidir el sentido del verbo de la acción penal. Además esta norma deja de lado un relevante aspecto, la acción de influir en el ingreso de los datos al sistema de cómputo. En dicho artículo se habla de la sanción a la influencia en el procesamiento o resultado de los datos pero nunca menciona la palabra ingreso. Se puede pensar que al hablar de la acción del procesamiento se asuma que esta incluido el aspecto incluir sin embargo resultaría muy superficial y alejado de la realidad del que hacer informático, pues el procesamiento del delito trata de la manipulación o alteración de los datos ya ingresados al sistema informático, como un paso posterior a ese olvidado ingreso.

Alteración de datos y sabotaje informático (artículo 229bis)

Esta última norma nos dice: "Se impondrá prisión de uno a cuatro años a la persona que por cualquier medio accese, borre, suprima, modifique o inutilice sin autorización los datos

registrados en una computadora". Además agrega si como resultado de las conductas indicadas se entorpece o inutiliza el funcionamiento de un programa de cómputo, una base de datos o el sistema informático, la pena será de tres a seis años de prisión. Si el programa de cómputo, la base de datos o el sistema informático contienen datos de carácter público, se impondrá pena de prisión hasta de ocho años. (código penal, 1971)

En dicho artículo se está penalizando por una infracción de peligro abstracto ya que con solo el hecho de acceder a un sistema sin autorización hace surgir la responsabilidad penal. La norma además agrega una figura agravada al indicar que la pena será mayor en caso de que sean datos de carácter público y se entorpece o inutiliza su funcionamiento; es bueno que se resalte este tipo de agravantes, sin embargo se presenta un problema, la pena dice que puede ser hasta de ocho años de prisión, no obstante, no habla de un mínimo de penalidad, por lo que una persona podría tener una pena inferior a los tres años si se juzga bajo la norma agravada por lo que resultaría mejor juzgarlo con un proceder no agravado pues así podría cumplir un mínimo de tres años de prisión.

Por ejemplos como el caso anterior es que la finalidad que pudo perseguirse en cuanto a describir una conducta agravada por la afectación de datos de carácter público, con la aplicación de una sanción mayor no se logró correctamente, y puede presentarse para una distorsión del sistema.

La reforma al código penal por la ley Nº 8148, en la que se incorporan tres figuras de delitos informáticos, responde, sin duda, a la imperiosa necesidad de actualizar nuestro

sistema penal a los avances informáticos, en la cual la criminalidad está en pleno desarrollo y posee un decisivo impacto social.

Por otro lado estos tres delitos abren las puertas a futuras reformas, tal es el caso del proyecto del año 1996 de reforma al código penal en el que se incluían por primera vez, la creación de varios delitos informáticos, sin embargo no tuvo eco en ese momento por lo que fue desechada. Esta propuesta fue retomada por el poder ejecutivo en el año 1998 bajo la ley Nº11.871 pero esta propuesta también fracasó y se quedó en el olvido.

Para el año 2002, la corte suprema de justicia retomó el proyecto de reforma integral del código penal nuevamente y lo presentó a conocimiento de la asamblea legislativa para su estudio. Dicho proyecto tiene el mismo número de ley que el anterior intento 11.871 y actualmente se encuentra en discusión en la comisión de asuntos jurídicos de la asamblea legislativa.

En dicho proyecto se habla de artículos como tratamiento ilícito de datos personales y comunicaciones (artículo 179 del proyecto), uso ilícito de registros informáticos (artículo 181 del proyecto), hurto informático agravado (artículo 226, incisos 3 y 8), fraude informático (artículo 240 del proyecto), daño informático agravado (artículo 249, inciso 6 del proyecto).

Conclusión

El panorama en cuanto a los delitos informáticos, como se pudo notar, es muy amplio. Hoy en día gracias al avance de la tecnología contamos con las herramientas básicas para saber cuando nos encontramos ante una conducta criminal informática y además de las características que debemos buscar en el autor de tales hechos delictivos para identificarlo como tal.

El estudio de una gran variedad de delitos informáticos permite tener un mejor criterio sobre la gravedad de la criminalidad informática y su falta de regulación eficaz. Las legislaciones de los diferentes países se quedan cortas en su regulación, pero más complejo sería pensar en normas de carácter internacional que penalicen las conductas consideradas como graves, no porque no sea lo más conveniente, sino por los problemas de la naturaleza jurídica de los diferentes sistemas penales, así como por los intereses particulares en asuntos de política criminal de cada uno de los países, no se presta para actuar de una forma rápida y efectiva.

Día a día podemos ir conociendo nuevas formas de delincuencia informática, pero como siempre suele suceder, la realidad camina delante del sistema penal, en el que se aprecia un notable letargo en la conformación de normas que regulen esas novedosas conductas como delito. Sin embargo, no por eso podemos dejar nuestra sociedad al servicio de los delincuentes informáticos; nuestra legislación debe actualizarse y ponerse a tono con la del resto del mundo, eso es un hecho, la experiencia de otras naciones resultará muy importante

para adelantar el conocimiento de consecuencias perjudiciales que desgraciadamente muy pronto tendremos en nuestro país.

La tarea ya se ha iniciado, pero todavía falta caminar un gran trayecto y librar una gran lucha para convencer principalmente a nuestros legisladores sobre los graves impactos que pueden traer consigo los delitos informáticos, los cuales no tienen fronteras. En nuestros hombros se encuentra el futuro inmediato; es por eso que debemos actuar ahora mismo conociendo más el medio que nos rodea para garantizar a las futuras generaciones su sobrevivencia en una adecuada calidad de vida.

Por todo lo expuesto, se puede decir que el reto está sobre la mesa; en cada uno de nosotros queda el tomar la palabra y actuar en forma correcta.

Bibliografía

Amoroso Fernandez, Yarina. (1998) Contribución al debate sobre la conveniencia de una legislación en internet. *Informática y derecho: delito cibernético,27-28-29,* setiembre, p. 73-111.

Barceló García, Miguel. (1993) *El fraude y la delincuencia informática un problema jurídico y ético*. *El derecho penal,10,* julio, p. 31-54.
Gomez Perals, Miguel. (1994) Los delitos informáticos en el derecho español. *Informática y derecho: delito cibernético,5-6,* febrero, p. 481-496.

Benedito, José. (1998) Hacia la sociedad de la información. *Informática y derecho: delito cibernético,27-28-29,* setiembre, p. 233-251.

Cancino Moreno, Antonio José. (1998) Es necesario crear en el código penal un capítulo para los denominados delitos informáticos. *Colegio de abogados penalistas del valle,19,* mayo, p. 111-130.

Carrascosa Lopez, Valentin. (1998) Es necesario una legislación mundial por internet. *Informática y derecho: delito cibernético,27-28-29,* setiembre, p. 161-181.

Chinchilla Sandí, Carlos. (2004) *Delitos informáticos*. Costa Rica: Farben.

Correa, Carlos Maria. (1987) *Derecho informático*. España.

Estrada Posada, Rodolfo; Somellera, Roberto. (1998) Delios informáticos. *Informática y derecho: delito cibernético,27-28-29,* setiembre, p. 423-441.

Guerra de Villaláz, Aura E. (1993) *Derecho penal:están tipificados los delitos informáticos en la legislación panameña*. Panamá: Litho.

Madriz Vargas, Carmen. (2002) *Persecución penal de los delitos informáticos*. Costa Rica: Tesis.

Ribas, Alejandro Javier. (1998) La sociedad digital: riesgos y oportunidades. *Informática y derecho: delito cibernético,27-28-29,* setiembre, p. 51-61.

Rojas Jiménez, Oscar. (1995) *La informática y los problemas en materia de calificación delictual*. México: Farben.

Romero Casabona, Carlos María. (1993) Tendencias actuales sobre las formas de protección jurídica ante las nuevas tecnologías. *Poder Judicial,31,* setiembre, p.163.

Salazar, Alonso. (2001) *Analisis comparativo con el delito de daños y otros tipos en el código penal costarricense*. Costa Rica: Farben.

Sanchez Delgado, Daniel. (1997) La estafa, análisis de sus elementos y problemática con los llamados delitos informáticos. *Judicial,65,* noviembre, p. 53-80.

Tellez Valdez, Julio. (1996) Los delitos informáticos: situación enMéxico. *Informática y derecho: delito cibernético,9-10-11,* marzo, p. 461-473.