Mayo 2009

LOS DELITOS INFORMÁTICOS. TRATAMIENTO INTERNACIONAL

MsC. Egil Emilio Ramírez Bejerano
Lic. Ana Rosa Aguilera Rodríguez

Para citar este artículo puede utilizar el siguiente formato:

Ramírez Bejerano y Aguilera Rodríguez: *Los delitos informáticos. Tratamiento internacional,* en Contribuciones a las Ciencias Sociales, mayo 2009. www.eumed.net/rev/cccss/04/rbar2.htm

ÍNDICE

RESUMEN

Indiscutiblemente continúa siendo el Derecho la principal fuente inagotable de adaptación social en la Comunidad Mundial de Naciones. Resulta fantástico apreciar como la Humanidad ha ido insertando los adelantos científico-tecnológicos en aras de perfeccionar los principales mecanismos de comunicación y avances hacia el desarrollo. El uso imprescindible de las nuevas técnicas de la información implica además un seguimiento continuo a conductas que transgreden la voluntad política de los Estados Nacionales y, en su caso, la respuesta punitiva de quien es, junto al Estado, la más antigua y necesaria institución mundial.

La estructura orgánica del trabajo que se presenta está dividida en análisis teórico-prácticos de los principales aspectos doctrinales que avalan el amplio proceso de formación, desarrollo, proyección y protección de los delitos informáticos. Un singular esquema de referencias completan, con detallada sencillez los mecanismos internacionales que desde sus inicios buscan mancomunadamente soluciones fehacientes a las enormes problemáticas, peligros y amenazas que enfrenta la Humanidad.

Se realiza un análisis de las principales causas que generaron y condicionaron la evolución de los delitos informáticos, sus entes de referencia, clasificación, seguimiento internacional en las legislaciones de un grupo de países del mundo desarrollado y sub-desarrollado, así como los principales elementos doctrinales que la Comunidad Mundial tiene en consideración en aras de darle un tratamiento efectivo con ayuda de los organismos internacionales y el apoyo incondicional de los Estados Nacionales.

Se abunda además en el papel protagónico de nuestra América y su toma de acción en los agobiantes problemas que mueven la realidad latina de hoy, tomando como punto de conexión tres países del área, abordando sus sujetos pasivos y activos, elementos imprescindibles si se tienen en cuenta las consecuencias que traería la proliferación de esta especie jurídica.

Se analizan además, como resultado de un minucioso y exhaustivo análisis, las principales problemáticas que, a juzgar por las Naciones Unidas, deben tomarse de la mano, y ejecutarse como parte de una serie de acciones concretas, con el objetivo de hacer frente a las regulaciones específicas del uso del correo electrónico, la pornografía infantil en Internet.

RESUMEN

Unquestionably it continues being the Right the main inexhaustible source of social adaptation in the World Community of Nations. It is fantastic to appreciate as the Humanity he/she has gone inserting the scientific-technological advances for the sake of perfecting the main communication mechanisms and advances toward the development. The indispensable use of the new techniques of the information also implies a continuous pursuit to behaviors that transgress the political will of the National States and, in its case, the punitive answer of who is, next to the State, the oldest and necessary world institution.

The organic structure of the work that is presented is divided in theoretical-practical analysis of the main doctrinal aspects that endorse the wide formation process, development, projection and protection of the computer crimes. A singular outline of references completes, with detailed simplicity the international mechanisms that look for conjointly from their beginnings solve fehacientes to the enormous ones problematic, dangers and threats that the Humanity faces.

2. INTRODUCCIÓN

"Los Delitos Informáticos. Tratamiento Internacional: Doctrina y práctica" es nuestro tema de análisis y uno de los aspectos doctrinales que avalan el Sistema de Protección Mundial a esta nueva figura jurídica en la Comunidad Mundial de Naciones, quienes han insertado los principios de las Naciones Unidas en su política de protección y utilización a las nuevas tecnologías y servicios informáticos.

El desarrollo de las tecnologías informáticas ofrece un aspecto negativo: Ha abierto la puerta a conductas antisociales y delictivas. Los sistemas de computadoras ofrecen oportunidades nuevas y sumamente complicadas para infringir la ley y han creado la posibilidad de cometer delitos de tipo tradicional en formas no tradicionales.

Bajo esta perspectiva, los organismos internacionales que integran el engranaje de la Comunidad Mundial, realizan mancomunados esfuerzos en aras de viabilizar

una serie de proyectos que en coordinación con la voluntad de los Estados Nacionales pueden materializarse en un período corto cargado de optimismo.

La estructura doctrinal de nuestro estudio comprende aspectos metodológicos concernientes a la evolución de los delitos informáticos y su regulación jurídica ya no solo en un grupo de países, sino en el entorno legislativo que rodea la Comunidad Mundial, siento esta última, en el amplio orden de ideas que mueven la palabra, la más afectada por este flagelo.

Los principales delitos reconocidos por las Naciones Unidas, su comportamiento y trasgresión de las normas internacionales del Derecho, clasificación, ideas reguladoras, el acceso a Internet de los menores en el peligroso marco de pornografía infantil que trasciende los marcos de fenómeno social, el uso adecuado de las principales normativas para acceder al correo electrónico, entre otros aspectos de interés son sin duda algunas de las propuestas que con detallada sencillez profesional, se persiguen.

Es objetivo de este trabajo analizar, las conductas delictivas que pueden generar el gran avance tecnológico, sobre todo en el campo de la informática" desde tres de puntos de vista: normativo, delincuencia y prevención.

CAPÍTULO I: INTRODUCCIÓN A LOS DELITOS INFORMÁTICOS

1.1. Complementación teórica

A lo largo de la historia el hombre ha necesitado transmitir y tratar la información de forma continua. Aun están en el recuerdo las señales de humo y los destellos con espejos, y más recientemente los mensajes transmitidos a través de cables utilizando el código Morse, o la propia voz por medio del teléfono. La humanidad no ha cesado en la creación de métodos para procesar información. Con ése fin nace la informática, como ciencia encargada del estudio y desarrollo de éstas máquinas y métodos, y además con la idea de ayudar al hombre en aquellos trabajos rutinarios y repetitivos, generalmente de cálculo o de gestión.

Luego nace Internet como una tecnología que pondría la cultura, la ciencia y la información al alcance de millones de personas de todo el mundo. Delincuentes diversos encontraron el modo de contaminarla y lo que es peor, hacerlo impunemente. La contaminación es de la más variada, entre los últimos ataques a la red que pueden calificarse como de los más graves es el uso de la red por parte de la mafia internacional que maneja la prostitución infantil, por el terrorismo internacional y también por el narcotráfico. Políticos de algunos países han pedido que se reglamente el uso de la red, de modo que quienes prestan el servicio de Internet registren a los clientes, cuando y donde llaman y para que, pero la iniciativa hizo que, en defensa de la libertad y de la privacidad, muchos usuarios honestos y algunas empresas que participan de los beneficios económicos de la red, protestaran enérgicamente. Sin embargo, debe destacarse que el uso de las técnicas informáticas ha creado nuevas posibilidades del uso indebido de las computadoras lo que ha propiciado a su vez la necesidad de regulación por parte del derecho. El espectacular desarrollo de la tecnología informática ha abierto las puertas a nuevas posibilidades de delincuencia antes impensables. La manipulación fraudulenta de los ordenadores con ánimo de lucro, la destrucción de programas o datos y el acceso y la utilización indebida de la información son algunos de los principales retos que cercan el mundo contemporáneo.

1.2. Los delitos informáticos: Conceptualización

No hay definición de carácter universal propia de delito Informático, sin embargo muchos han sido los esfuerzos de expertos que se han ocupado del tema, y aun cuando no existe una definición con carácter universal, se han formulado conceptos funcionales atendiendo a realidades nacionales concretas. En el ámbito internacional se considera que no existe una definición propia del *delito informático*, sin embargo al consultar la bibliografía internacional, específicamente al insigne estudioso español Carlos Sarzana, en su obra Criminalitá e tecnología, los crímenes

por computadora comprenden "Cualquier comportamiento criminógeno en el cual la computadora ha estado involucrada como material o como objeto de la acción criminógena, o como mero símbolo".

A continuación mostramos los criterios doctrinales de algunos tratadistas al respecto:
* Nidia Callegari define al "delito Informático" como "aquel que se da con la ayuda de la informática o de técnicas anexas".
* Rafael Fernández Calvo define al "delito Informático" como la realización de una acción que, reuniendo las características que delimitan el concepto de delito, se ha llevado a cabo utilizando en elemento informático o telemático contra los derechos y libertades de los ciudadanos definidos en el título 1 de la Constitución Española"
*María de la Luz Lima dice que el "delito electrónico" "en un sentido amplio es cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin y que, en un sentido estricto, el delito Informático, es cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como método, medio o fin"
*Julio Téllez Valdés conceptualiza al "delito Informático" en forma típica y atípica, entendiendo por la primera a "las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin" y por las segundas "actitudes ilícitas en que se tienen a las computadoras como instrumento o fin"

Por otra parte, debe mencionarse que se han formulado diferentes denominaciones para indicar las conductas ilícitas en las que se usa a la computadora, tales como "delitos informáticos", "delitos electrónicos", "delitos relacionados con la computadora", "crímenes por computadora", delincuencia relacionada con el ordenador". Analizando estas determinaciones conceptuales estamos en condiciones de brindar una definición de ***delito informático***:

Son todas aquellas conductas ilícitas susceptibles de ser sancionadas por el derecho penal, que hacen uso indebido de cualquier medio Informático implicando actividades criminales.

1.3 Clasificación

Según Oliver Hance en su libro “Leyes y Negocios en Internet”, existen tres categorías de comportamiento que pueden afectar negativamente a los usuarios de los sistemas informáticos: Acceso no autorizado, actos dañinos o circulación de material dañino e intercepción no autorizada. Las leyes estadounidense y canadiense, lo mismo que los sistemas legales de la mayoría de los países europeos han tipificado y penado y penalizado estos tres tipos de comportamiento, ilícito. Muchos autores han abordado el tema con singular pasión, clasificando a los delitos informáticos sobre la base de dos criterios: como instrumento o medio, o como fin u objetivo.

Como instrumento o medio: Se tienen a las conductas criminógenas que se valen de las computadoras como método, medio, o símbolo en la comisión del ilícito. *Como fin u objetivo*: En ésta categoría se enmarcan las conductas criminógenas que van dirigidas en contra de la computadora, accesorios o programas como entidad física. Otros sin embargo advierten una clasificación sui géneris, "delitos electrónicos" diciendo que existen tres categorías, a saber:
Los que utilizan la tecnología electrónica como método (Conductas criminógenas en donde los individuos utilizan métodos electrónicos para llegar a un resultado ilícito).
Los que utilizan la tecnología electrónica como medio (Conductas criminógenas en donde para realizar un delito utilizan una computadora como medio o símbolo) y, *Los que utilizan la tecnología electrónica como fin* (conductas criminógenas dirigidas contra la entidad física del objeto o máquina electrónica o su material con objeto de dañarla) Ahora bien realicemos un análisis objetivo de estas clasificaciones a los delitos informáticos: como instrumento o medio, o como fin u objetivo.

1. Como instrumento o medio

- Se tienen a las conductas criminógenas que se valen de las computadoras como método, medio, o símbolo en la comisión del ilícito.

2. Como fin u objetivo
    - En esta categoría se enmarcan las conductas criminógenas que van dirigidas en contra de la computadora, accesorios o programas como entidad física.

1. 1. Los que utilizan la tecnología electrónica como método,
2. 2. Los que utilizan la tecnología electrónica como medio y
3. 3. Los que utilizan la tecnología electrónica como fin.

Como método- conductas criminógenas en donde los individuos utilizan métodos electrónicos para llegar a un resultado ilícito.

Como medio.- conductas criminógenas en donde para realizar un delito utilizan una computadora como medio o símbolo.

Como fin.- conductas criminógenas dirigidas contra la entidad física del objeto o máquina electrónica o su material con objeto de dañarla.

1.4 Sujeto activo

Las personas que cometen los "Delitos Informáticos" son aquellas que poseen ciertas características que no presentan el denominador común de los delincuentes. Los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso de los sistemas informatizados, aún cuando en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos.

Con el tiempo se ha podido comprobar que los autores de los delitos informáticos son muy diversos y que lo que los diferencia entre sí es la naturaleza de los delitos cometidos. De esta forma, la persona que "entra" en un sistema Informático sin intenciones delictivas es muy diferente del empleado de una institución financiera que desvía fondos de las cuentas de sus clientes. El nivel típico de aptitudes del delincuente Informático es tema de controversia ya que para algún dicho nivel no es indicador de delincuencia informática en tanto que otros aducen que los posibles delincuentes informáticos son personas listas, decididas, motivadas y dispuestas a aceptar un reto tecnológico, características que pudieran encontrarse en un empleado del sector de procesamiento de datos. Sin embargo, teniendo en cuenta las características ya mencionadas de las personas que cometen los "delitos informáticos", estudiosos en la materia los han catalogado como "delitos de cuello blanco" término introducido por primera vez por el criminólogo norteamericano Edwin Sutherland en el año 1943. Efectivamente, este conocido criminólogo señala un sinnúmero de conductas que considera como "delitos de cuello blanco", aún cuando muchas de estas conductas no están tipificadas en los ordenamientos jurídicos como delitos, y dentro de las cuales cabe destacar las "violaciones a las leyes de patentes y fábrica de derechos de autor, el mercado negro, el contrabando en las empresas, la evasión de impuestos, las quiebras fraudulentas, corrupción de altos funcionarios, entre otros". Asimismo, este criminólogo estadounidense dice que tanto la definición de los "delitos informáticos" como la de los "delitos de cuello blanco" no es de acuerdo al interés protegido, como sucede en los delitos convencionales sino de acuerdo al sujeto activo que los comete. Entre las características en común que poseen ambos delitos tenemos que: el sujeto activo del delito es una persona de cierto status socioeconómico, su comisión no puede explicarse por pobreza ni por mala habitación, ni por carencia de recreación, ni por baja educación, ni por poca inteligencia, ni por inestabilidad emocional. Es difícil elaborar estadísticas sobre ambos tipos de delitos. La "cifra negra" es muy alta; no es fácil descubrirlo y sancionarlo, en razón del poder económico de quienes lo cometen, pero los daños económicos son altísimos; existe una gran indiferencia de la opinión pública sobre los daños ocasionados a la sociedad; ésta no considera delincuentes a los sujetos que cometen este tipo de delitos, no los segrega, no los desprecia, ni los desvaloriza, por el contrario, el autor o autores de este tipo de delitos se considera a sí mismos "respetables". Otra coincidencia que tienen estos tipos de delitos es que, generalmente, son objeto de medidas o sanciones de carácter administrativo y no privativos de la libertad.

Por nuestra parte, consideramos que a pesar de que los "delitos informáticos" no poseen todas las características de los "delitos de cuello blanco", si coinciden en un número importante de ellas, aunque es necesario señalar que estas aseveraciones pueden y deben ser objetos de un estudio más profundo. El nivel típico de aptitudes del delincuente informático es tema de controversia ya que para algunos el nivel de aptitudes no es indicador de delincuencia informática en tanto que otros aducen que los posibles delincuentes informáticos son personas listas, decididas, motivadas y dispuestas a aceptar un reto tecnológico, características que pudieran encontrarse en un empleado del sector de procesamiento de datos.

1.5 sujeto pasivo

En primer término tenemos que distinguir que *sujeto pasivo o víctima* del delito es el ente sobre el cual recae la conducta de acción u omisión que realiza el sujeto activo, y en el caso de los "*delitos informáticos*" las víctimas pueden ser individuos, instituciones crediticias, gobiernos, etcétera que usan sistemas automatizados de información, generalmente conectados a otros. El sujeto pasivo del delito que nos ocupa, es sumamente importante para el estudio de los "*delitos informáticos"*, ya que mediante él podemos conocer los diferentes ilícitos que cometen los delincuentes informáticos, con objeto de prever las acciones antes mencionadas debido a que muchos de los delitos son descubiertos casuísticamente por el desconocimiento del modus operandi de los sujetos activos. Es importante puntualizar que ha sido imposible conocer la verdadera magnitud de los "delitos informáticos", ya que la mayor parte de los delitos no son descubiertos o no son denunciados a las autoridades responsables y si a esto se suma la falta de leyes que protejan a las víctimas de estos delitos; la falta de preparación por parte de las autoridades para comprender, investigar y aplicar el tratamiento jurídico adecuado a esta problemática; el temor por parte de las empresas de denunciar este tipo de ilícitos por el desprestigio que esto pudiera ocasionar a su empresa y las consecuentes pérdidas económicas, entre otros más, trae como consecuencia que las estadísticas sobre este tipo de conductas se mantenga bajo la llamada "cifra oculta" o "cifra negra". Por lo anterior, se reconoce que para conseguir una prevención efectiva de la criminalidad informática se requiere, en primer lugar, un análisis objetivo de las necesidades de protección y de las fuentes de peligro. Una protección eficaz contra la criminalidad informática presupone ante todo que las víctimas potenciales conozcan las correspondientes técnicas de manipulación, así como sus formas de encubrimiento. En el mismo sentido, podemos decir que mediante la divulgación de las posibles conductas ilícitas derivadas del uso de las computadoras, y alertando a las potenciales víctimas para que tomen las medidas pertinentes a fin de prevenir la delincuencia informática, y si a esto se suma la creación de una adecuada legislación que proteja los intereses de las víctimas y una eficiente preparación por parte del personal encargado de la procuración, administración y la impartición de justicia para atender e investigar estas conductas ilícitas, se estaría avanzando mucho en el camino de la lucha contra la delincuencia informática, que cada día tiende a expandirse más.

Además, se debe destacar que los organismos internacionales han adoptado resoluciones similares en el sentido de que educando a la comunidad de víctimas y estimulando la denuncia de los delitos se promovería la confianza pública en la capacidad de los encargados de hacer cumplir la ley y de las autoridades judiciales para detectar, investigar y prevenir los delitos informáticos**.**

1.6 Panorama mundial

Un ejemplo clarificador es lo que ocurrió con el famoso *gusano* de Internet que lanzó Robert Morris Jr. en noviembre de 1988 y que acabó bloqueando más de 6 000 ordenadores: De no existir en ese momento el Acta sobre Fraude y Abuso Informático en Estados Unidos, es más que dudoso que se le hubiese podido juzgar.

Hay que recordar también que las compañías de seguros, de varios países, ofrecen cobertura concreta contra este tipo de delitos. Sólo en Estados Unidos se calcula que se generan perjuicios económicos, por los delitos informáticos, que superan los 10.000 millones de dólares o más de 5.000 millones de libras esterlinas en el Reino Unido. También hay que recordar que hasta la propia Dirección General de Policía en España, al igual que muchos otros países, ha tenido que crear un Grupo dedicado en exclusiva a los delitos informáticos.

Casi el 90% de los delitos informáticos que investiga el FBI en Estados Unidos tienen que ver con Internet. Esto nos enlaza directamente con los problemas de inexistencia de fronteras que aparecen constantemente cuando tratamos estos delitos: ¿Cuál es la ley a aplicar en multitud de casos? La solución pasa por una coordinación internacional, tanto a la hora de investigar como a la hora de aplicar unas leyes que deben contar con un núcleo común. Es decir, hay que unificar criterios: difícil será actuar contra un delito que sí lo es en un país y no en otro. En este sentido está trabajando, por ejemplo, la Unión Europea. Es cierto, de todas formas, que un delito informático puede ser simplemente un *delito clásico* en un nuevo envoltorio. Lo que ocurre es que no sólo es eso. Además el avance que está sufriendo Internet en número de usuarios, que parece que vaya a colapsarse en cualquier momento, y en broma se hable ya del ciberespacio, hace que haya que actuar rápidamente ante los posibles delitos que puedan cometerse a través de ella: con el aumento de la ciberpoblación, aumentan los posibles delincuentes y los posibles objetivos.

Muchas empresas que en un principio no querían conectarse a Internet, precisamente por los posibles problemas de seguridad, ahora no quieren quedarse atrás, ya que se ha convertido en una cuestión o de pura necesidad o de imagen, y ahora se conectan a marchas forzadas, lo que hace que muchas no tomen las precauciones necesarias y se conviertan automáticamente en jugosos y fáciles objetivos. Internet no estaba pensada y desarrollada para lo que está ocurriendo: su propio diseño no está basado sobre protocolos híper-seguros y, tan es así, que hoy dia se estima que no existe un sólo servidor en el mundo que no haya sufrido un ataque contra su seguridad por parte de hackers y crackers. Desde el punto de vista de la seguridad también es preocupante el uso de la criptología por parte de los delincuentes, tanto para ocultar sus mensajes haciéndolos ininteligibles, como para ocultar sus propios movimientos en un sistema informático, haciendo que incluso aunque sean detectados no se pueda saber exactamente que es lo que estaban haciendo, al estar encriptados los archivos descubiertos. En este sentido, actualmente es muy inquietante la utilización de cripto-virus (programas con código vírico encriptados). Lógicamente, no es que la criptología sea mala en sí (presenta más ventajas que desventajas): el problema surge cuando es utilizada por *malas manos*.

En el **nuevo Código Penal español** (aprobado por Ley-Orgánica 10/1995, de 23 de noviembre / BOE número 281, de 24 de noviembre de 1995) hay varios artículos íntimamente relacionados con el tema que estamos tratando, un ejemplo es:
1.- El que para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses. Al respecto, según un estudio publicado en el manual de las Naciones Unidas en la prevención y control de los delitos informáticos (# 43 y # 44) el 90% de los delitos realizados mediante la computadora fueron ejecutados por empleados de la misma empresa afectada. Asimismo, otro creciente realizado en América Latina y Europa indicó que el 73% de las intrusiones cometidas eran atribuibles a fuentes interiores y solo el 23% a la actividad externa.

CAPÍTULO II: TRATAMIENTO INTERNACIONAL

2.1 Tratados Internacionales

En los últimos años se ha perfilado en el ámbito internacional un cierto consenso en las valoraciones político-jurídicas de los problemas derivados del mal uso que se hace de las computadoras, lo cual ha dado lugar a que, en algunos casos, se modifiquen los derechos penales nacionales.

El GATT, se transformó en lo que hoy conocemos como la Organización Mundial de Comercio (OMC), por consecuencia todos los acuerdos que se suscribieron en el marco del GATT, siguen estando vigentes. En el Art. 61 se establece que para los casos de falsificación dolosa de marcas de fábrica o de comercio o de piratería lesiva del derecho de autor a escala comercial se establecerán procedimientos y sanciones penales además de que "Los recursos disponibles comprenderán la pena de prisión y/o la imposición de sanciones pecuniarias suficientemente disuasorias"
*El convenio de Berna
*La convención sobre la Propiedad Intelectual de Estocolmo
*La Convención para la Protección y Producción de Fonogramas de 1971
*La Convención Relativa a la Distribución de Programas y Señales

En 1983 la Organización de Cooperación y Desarrollo Económico (OCDE) inició un estudio de la posibilidad de aplicar y armonizar en el plano internacional las leyes penales, a fin de luchar contra el problema del uso indebido de los programas de computación. Las posibles implicaciones económicas de la delincuencia informática tienen carácter internacional e incluso transnacional, cuyo principal problema es la falta de una legislación unificada que, facilita la comisión de los delitos. En 1986 la OCDE publico un informe titulado Delitos de informática: análisis de la normativa jurídica, donde se reseñaban las normas legislativas vigentes y las propuestas de reforma en diversos Estados miembros y se recomendaba una lista mínima de ejemplos de uso indebido que los países podrían prohibir y sancionar en leyes penales. En 1992 elaboró un conjunto de normas para la seguridad de los sistemas de información, con intención de ofrecer las bases para que los Estados y el sector privado pudieran erigir un marco de seguridad para los sistemas informáticos. En 1990 la Organización de las Naciones Unidas (ONU) en el Octavo Congreso sobre Prevención del Delito y Justicia Penal, celebrado en La Habana, Cuba, se dijo que la delincuencia relacionada con la informática era consecuencia del mayor empleo del proceso de datos en las economías y burocracias de los distintos países y que por ello se había difundido la comisión de actos delictivos. La ONU ha publicado una descripción de "Tipos de Delitos Informáticos", que se transcribe al final de ésta sección. En 1992 La Asociación Internacional de Derecho Penal durante el coloquio celebrado en Wurzburgo en 1992, adoptó diversas recomendaciones respecto a los delitos informáticos, entre ellas que, en la medida que el derecho Penal no sea suficiente, deberá promoverse la modificación de la definición de los delitos existentes o la creación de otros nuevos, si no basta con la adopción de otras medidas como por ejemplo el "principio de subsidiariedad".

Hay otros Convenios no ratificados aún por nuestro País, realizados por la Organización Mundial de la Propiedad Intelectual (OMPI), de la que nuestro país es parte integrante a partir del 8/10/1980. En Noviembre de 1997 se realizaron las II Jornadas Internacionales sobre el Delito Cibernético en Mérida España, donde se desarrollaron temas tales como:
Aplicaciones en la Administración de las Tecnologías Informáticas / cibernéticas
Blanqueo de capitales, contrabando y narcotráfico
Hacia una policía Europea en la persecución del delito Cibernético.
Internet: a la búsqueda de un entorno seguro.
Marco legal y Deontológico de la Informática.

2.2. Legislación en otros países

Se ha dicho que algunos casos de abusos relacionados con la informática deben ser combatidos con medidas jurídico-penales. No obstante, para aprehender ciertos comportamientos merecedores de pena con los medios del Derecho penal tradicional, existen, al menos en parte, relevantes dificultades. Estas proceden en

buena medida, de la prohibición jurídico-penal de analogía y en ocasiones, son insuperables por la vía jurisprudencial. De ello surge la necesidad de adoptar medidas legislativas. En los Estados industriales de Occidente existe un amplio consenso sobre estas valoraciones, que se refleja en las reformas legales de los últimos diez años.

Pocos son los países que disponen de una legislación adecuada para enfrentarse con el problema sobre el particular, sin embargo con objeto de que se tomen en cuenta las medidas adoptadas por ciertos países, a continuación se presenta los siguientes casos particulares:

Alemania 

En Alemania, para hacer frente a la delincuencia relacionada con la informática y con efectos a partir del 1 de agosto de 1986, se adoptó la Segunda Ley contra la Criminalidad Económica del 15 de mayo de 1986 en la que se contemplan los siguientes delitos:

- Espionaje de datos (202 a)
- Estafa informática (263 a)
- Falsificación de datos probatorios(269) junto a modificaciones complementarias del resto de falsedades documentales como el engaño en el tráfico jurídico mediante la elaboración de datos, falsedad ideológica, uso de documentos falsos(270, 271, 273)
- Alteración de datos (303 a) es ilícito cancelar, inutilizar o alterar datos inclusive la tentativa es punible.
- Sabotaje informático (303 b. Destrucción de elaboración de datos de especial significado por medio de destrucción, deterioro, inutilización, eliminación o alteración de un sistema de datos. También es punible la tentativa.
- Utilización abusiva de cheques o tarjetas de crédito (266b).

Por lo que se refiere a la estafa informática, la formulación de un nuevo tipo penal tuvo como dificultad principal el hallar un equivalente análogo al triple requisito de acción engañosa, causa del error y disposición patrimonial, en el engaño del computador, así como en garantizar las posibilidades de control de la nueva expresión legal, quedando en la redacción que el perjuicio patrimonial que se comete consiste en influir en el resultado de una elaboración de datos por medio de una realización incorrecta del programa, a través de la utilización de datos incorrectos o incompletos, mediante la utilización no autorizada de datos, o a través de una intervención ilícita.

Sobre el particular, cabe mencionar que esta solución en forma parcialmente abreviada fue también adoptada en los Países Escandinavos y en Austria. En opinión de estudiosos de la materia, el legislador alemán ha introducido un número relativamente alto de nuevos preceptos penales, pero no ha llegado tan lejos como los Estados Unidos. De esta forma, dicen que no sólo ha renunciado a tipificar la mera penetración no autorizada en sistemas ajenos de computadoras, sino que tampoco ha castigado el uso no autorizado de equipos de procesos de datos, aunque tenga lugar de forma cualificada. En el caso de Alemania, se ha señalado que a la hora de introducir nuevos preceptos penales para la represión de la llamada criminalidad informática el gobierno tuvo que reflexionar acerca de dónde radicaban las verdaderas dificultades para la aplicación del Derecho penal tradicional a comportamientos dañosos en los que desempeña un papel esencial la introducción del proceso electrónico de datos, así como acerca de qué bienes jurídicos merecedores de protección penal resultaban así lesionados. Fue entonces cuando se comprobó que, por una parte, en la medida en que las instalaciones de tratamiento electrónico de datos son utilizadas para la comisión de hechos delictivos, en especial en el ámbito económico, pueden conferir a éstos una nueva dimensión, pero que en realidad tan sólo constituyen un nuevo modus operandi, que no ofrece problemas para la aplicación de determinados tipos. Por otra parte, sin embargo, la protección fragmentaria de determinados bienes jurídicos ha puesto de relieve que éstos no pueden ser protegidos suficientemente por el Derecho vigente contra nuevas formas de agresión que pasan por la utilización abusiva de instalaciones informáticas. En otro orden de ideas, las diversas formas de aparición de la

criminalidad informática propician además, la aparición de nuevas lesiones de bienes jurídicos merecedoras de pena, en especial en la medida en que el objeto de la acción puedan ser datos almacenados o transmitidos o se trate del daño a sistemas informáticos. El tipo de daños protege cosas corporales contra menoscabos de sus sustancias o función de alteraciones de su forma de aparición.

Austria 

Ley de reforma del Código Penal de 22 de diciembre de 1987
Esta ley contempla los siguientes delitos:

- Destrucción de datos (126). En este artículo se regulan no sólo los datos personales sino también los no personales y los programas.
- Estafa informática (148). En este artículo se sanciona a aquellos que con dolo causen un perjuicio patrimonial a un tercero influyendo en el resultado de una elaboración de datos automática a través de la confección del programa, por la introducción, cancelación o alteración de datos o por actuar sobre el curso del procesamiento de datos. Además contempla sanciones para quienes cometen este hecho utilizando su profesión.

Francia 

Ley número 88-19 de 5 de enero de 1988 sobre el fraude informático.

- Acceso fraudulento a un sistema de elaboración de datos(462-2).- En este artículo se sanciona tanto el acceso al sistema como al que se mantenga en él y aumenta la sanción correspondiente si de ese acceso resulta la supresión o modificación de los datos contenidos en el sistema o resulta la alteración del funcionamiento del sistema.
- Sabotaje informático (462-3).- En este artículo se sanciona a quien impida o falsee el funcionamiento de un sistema de tratamiento automático de datos.
- Destrucción de datos (462-4).- En este artículo se sanciona a quien intencionadamente y con menosprecio de los derechos de los demás introduzca datos en un sistema de tratamiento automático de datos o suprima o modifique los datos que este contiene o los modos de tratamiento o de transmisión.
- Falsificación de documentos informatizados (462-5).- En este artículo se sanciona a quien de cualquier modo falsifique documentos informatizados con intención de causar un perjuicio a otro.
- Uso de documentos informatizados falsos (462-6) En este artículo se sanciona a quien conscientemente haga uso de documentos falsos haciendo referencia al artículo 462-5.

Estados Unidos 

Consideramos importante mencionar la adopción en los Estados Unidos en 1994 del Acta Federal de Abuso Computacional (18 U.S.C. Sec.1030) que modificó al Acta de Fraude y Abuso Computacional de 1986. Con la finalidad de eliminar los argumentos hipertécnicos acerca de qué es y que no es un virus, un gusano, un caballo de Toya, etcétera y en que difieren de los virus, la nueva acta proscribe la transmisión de un programa, información, códigos o comandos que causan daños a la computadora, al sistema informáticos, a las redes, información, datos o programas (18 U.S.C.: Sec. 1030 (a) (5) (A). La nueva ley es un adelanto porque está directamente en contra de los actos de transmisión de virus. El Acta de 1994 diferencia el tratamiento a aquellos que de manera temeraria lanzan ataques de virus de aquellos que lo realizan con la intención de hacer estragos. El acta define dos niveles para el tratamiento de quienes crean virus estableciendo para aquellos que intencionalmente causan un daño por la transmisión de un virus, el castigo de hasta 10 años en prisión federal más una multa y para aquellos que lo transmiten sólo de manera imprudente la sanción fluctúa entre una multa y un año en prisión.

Nos llama la atención que el Acta de 1994 aclara que el creador de un virus no escudarse en el hecho que no conocía que con su actuar iba a causar daño a alguien o que él solo quería enviar un mensaje. En opinión de los legisladores estadounidenses, 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 se realicen. Diferenciando los niveles de delitos, la nueva ley da lugar a que se contemple qué se debe entender como acto delictivo. En el Estado de California, en 1992 se adoptó la Ley de Privacidad en la que se contemplan los delitos informáticos pero en menor grado que los delitos relacionados con la intimidad que constituyen el objetivo principal de esta Ley. Se considera importante destacar las enmiendas realizadas a la Sección 502 del Código Penal relativas a los delitos informáticos en la que, entre otros, se amplían los sujetos susceptibles de verse afectados por estos delitos, la creación de sanciones pecuniarias de $10, 000 por cada persona afectada y hasta $50,000 el acceso imprudente a una base de datos, etcétera.

El objetivo de los legisladores al realizar estas enmiendas, según se infiere, era la de 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. Asimismo, los legisladores consideraron que la proliferación de la tecnología de computadoras ha traído consigo la proliferación de delitos informáticos y otras formas no autorizadas de acceso a las computadoras, a los sistemas y las bases de datos y que la protección legal de todos sus tipos y formas es vital para la protección de la intimidad de los individuos así como para el bienestar de las instituciones financieras, de negocios, agencias gubernamentales y otras relacionadas con el estado de California que legalmente utilizan esas computadoras, sistemas y bases de datos. Es importante mencionar que en uno de los apartados de esta ley, se contempla la regulación de los virus (computer contaminant) conceptualizándolos aunque no los limita a un grupo de instrucciones informáticas comúnmente llamados virus o gusanos sino que contempla a otras instrucciones designadas a contaminar otros grupos de programas o bases de datos, modificar, destruir, copiar o transmitir datos o alterar la operación normal de las computadoras, los sistemas o las redes informáticas.

Holanda
El 1* de marzo de 1993 entró en vigor la Ley de los Delitos Informáticos, en la cual se penaliza el hancking, el preancking (utilización de servicios de telecomunicaciones evitando el pago total o parcial de dicho servicio), la ingeniería social (arte de convencer a la gente de entregar información que en circunstancias normales no entregaría), y la distribución de virus.

Reino Unido de la Gran Bretaña e Irlanda del Norte
Debido al caso de hancking en 1991, comenzó a regir la Computer Misuse Act, Ley de los abusos informáticos. Mediante esta ley el intento, exitoso o no de alterar datos informáticos es penado con hasta cinco años de prisión o multas. Pena además la modificación de datos sin autorización donde se incluyen los virus.

Venezuela
En el año 2001 se promulgó la Ley Especial contra los delitos Informáticos por Asamblea Nacional de la Republica Bolivariana de Venezuela.

De los Delitos Contra los Sistemas que Utilizan Tecnologías de Información, De los Delitos Contra la Propiedad, De los delitos contra la privacidad de las personas y de las comunicaciones, De los delitos contra niños, niñas o adolescentes, De los delitos contra el orden económico, argumentados en cinco capítulos respectivamente. En las disposiciones comunes se abordan elementos importantes como las agravantes, las penas accesorias, la divulgación de la sentencia condenatoria etc entre otros elementos.

Los Estados miembros de la Unión Europea acordaron castigar con penas de uno a tres años de prisión a los responsables de delitos informáticos. Cuando quede comprobado que los ataques cibernéticos están relacionados con el crimen organizado, la pena ascenderá hasta los cinco años. Esta decisión marco se convierte en un gran avance dentro de la armonización de las legislaciones

europeas para luchar contra los delitos informáticos. Estos delitos se han convertido en un quebradero de cabeza para los cuerpos de policía de los Estados miembros y, sobre todo, para los perjudicados por estos crímenes. El principio de territorialidad del derecho provoca que sea muy complicado perseguir a delincuentes informáticos que actúan desde otros países. Con este intento de unificar la legislación, las autoridades europeas podrán perseguir con una mayor efectividad a delincuentes que, hasta ahora, podían cometer sus delitos con casi total impunidad. Además, el acuerdo del Consejo de Ministros de Justicia de los Quince establece otro aspecto importante, como es la definición de los delitos que se consideran "informáticos". Los Estados miembros distinguen tres tipos de ataques *cibernéticos*: el acceso ilegal a sistemas informáticos, la ocupación de sistemas a través de ejemplos como el envío de mensajes que ocupan un espacio considerable, y la difusión de virus informáticos. La intención de la Unión Europea es doble: por un lado se trata de definir el delito; por otro pretende unificar las penas, ya que el lugar de la comisión del delito es fundamental para saber el derecho aplicable, se trata además de una medida muy sensata que evita la desprotección absoluta que presentan hoy en día las empresas del Viejo Continente. Los Quince Estados Europeos disponen ahora de un plazo de más de dos años para la adaptación de esta medida a sus textos legislativos.

CAPÍTULO III: LAS NACIONES UNIDAS Y LOS DELITOS INFORMÁTICOS

El Manual de las Naciones Unidas para la Prevención y Control de Delitos Informáticos señala que cuando el problema se eleva a la escena internacional, se magnifican los problemas y las insuficiencias, por cuanto, los delitos informáticos constituyen una forma de crimen trasnacional y su combate requiere de una eficaz cooperación concertada. Asimismo la ONU resume de la siguiente manera a los problemas que rodean a la cooperación internacional en el área de los delitos informáticos:

A) Falta de acuerdos globales acerca de que tipo de conductas deben constituir delitos informáticos.
B) Ausencia de acuerdos globales en la definición de dichas conductas delictivas.
C) Falta de especialización en las policías, fiscales y otros funcionarios judiciales en el campo de los delitos informáticos.
D) Falta de armonización entre las diferentes leyes procesales nacionales acerca de la investigación de los delitos informáticos.
E) Carácter trasnacional de muchos delitos cometidos mediante el uso de las computadoras.
F) Ausencia de tratados de extradición, de acuerdos de ayuda mutua y de mecanismos sincronizados que permitan la puesta en vigor de la cooperación internacional.

CONCLUSIONES

Después del estudio de las experiencias adquiridas por diferentes países al enfrentar el *delito informático* y la forma en que está siendo regulada esta problemática en el mundo, además del evidente incremento de esta situación, es necesario a pesar de que en el país el *delito informático* no ha alcanzado el grado de peligrosidad existente en esos países regular penalmente las conductas ilícitas derivadas del uso de la computadora, como más adelante expondremos.

En primer término, la difusión a las empresas, organismos, dependencias, particulares y a la sociedad en general, contribuirá notoriamente al nivel de concientización sobre el problema que nos ocupa. El siguiente paso será dar a conocer las medidas preventivas que se deben adoptar para evitar estas conductas ilícitas.

Dado el carácter trasnacional de los delitos informáticos mediante el uso de las computadoras se hace imprescindible establecer tratados de extradición o acuerdos de ayuda mutua entre los países que permitan fijar mecanismos más efecti-

vos para la puesta en vigor de instrumentos de cooperación internacional para contrarrestar eficazmente la incidencia de la criminalidad informática.

BIBLIOGRAFÍA

1. Acta Federal de Abuso Computacional de Estados Unidos de 1994.
2. Boletín Informático 10-19. Delitos Informáticos.com
3. Convenio sobre cibercrimen del Consejo Europeo de 23 de noviembre de 2001.
4. Ley Especial sobre los Delitos Informáticos de Venezuela de 2001.
5. Ley de los Abusos Informáticos de Gran Bretaña de 1992.
6. Ley número 88-19 de 1988 sobre el fraude informático en Francia.
7. Ley de reforma del Código Penal de 1987 en Austria.
8. Ley de los Delitos Informáticos de 1993 en Holanda.
9. Segunda Ley contra la Criminalidad Económica de 1986 en Alemania.
10. Boletín de las Naciones Unidas sobre los delitos informáticos de 2002.