Delitos Informáticos

RODOLFO ESTRADA POSADA
ROBERTO SOMELLERA

Instituto Tecnológico y de Estudios Superiores de Monterrey. Campus Estados de México

Aun paso de entrar al siglo XXI contamos con un sin número de adelantos científicos y tecnológicos que jamas nos hubiéramos podido imaginar, en este fin de siglo la informática es algo ya indispensable para nuestro diario funcionamiento ya que pasó de ser una herramienta de apoyo a un elemento básico en el accionar de toda la humanidad, con toda la información que se necesita manejar en nuestros tiempos sin la ayuda de los sistemas de computo y de las grandes computadoras nos seria imposible almacenar y organizarla, pero este progreso que en ocasiones resulta desbocado lleva consigo grandes ventajas a las que no estaríamos dispuestos a renunciar ya que son parte indispensable de nuestra vida diaria, pero como todo tiene un precio el que tenemos que pagar por toda este manejo de información es la de los delitos informáticos, que se dan a diario en cualquier país del mundo, desde el más pequeño hasta el más revolucionado. El campo de la informática se ve seriamente afectado por el mal manejo de la información que llega hasta donde nunca se imaginó el ser humano que podía llegar, en estos días el límite de la delincuencia informática es la imaginación. Los delitos en los que se incurren diariamente son e producto del mal empleo de los avances informáticos y de los sistemas de información , este mal empleo se incrementa a la vez que progresa la tecnología, ya que esta se utiliza para destruir en lugar de crear.

Estos delitos de tipo informático necesitan una regulación de tipo normativo, donde se debe evaluar su alcance y el daño que es causado al delinquir, un delito de este tipo por lo general produce grandes consecuencias que afectan a más de una persona, debido a que se afectan bases de datos e información que es compartida por un determinado número de usuarios, y esta información a su vez es compartida con usuarios de un segundo nivel y así sucesivamente hasta que se llega al usuario final que es el último en participar en la cadena de destrucción , perdida o modificación de la información. Es necesario frenar este tipo de actos delictivos, antes que alcancen niveles incontrolables por las mismas autoridades, para esto es necesario que se vuelva homogéneo todo lo que se refiere al delito informático, ya que se tienen diferentes acepciones del concepto y el primer paso en México sería el estandarizar este hecho, para lo que se necesitaría una participación de gran parte de la sociedad informática, donde se trabajaría en conjunto con los órganos legislativos.

En la actualidad se cuenta dentro de la ley con distintas leyes que protegen de cierta manera pero muy ambigua a los productores de sistemas de información y en general a los autores intelectuales de los programas de computo. Como es el caso de la Ley federal de los derechos de Autor y el Código Penal para el Distrito Federal en Materia de Fuero Común y para toda la República en Materia de Fuero Federal, pero en estricto sentido estas normas no regulan los delitos informáticos, únicamente sancionan acciones que impliquen a la propiedad intelectual sin especificar que se trate de un programa de computo, y que debido a su naturaleza no pueden ser tratados de la misma manera, por poseer características totalmente distintas.

Si el espacio cibernético es tomado como un tipo de comunidad, un gigantesco vecindario formado por un número ilimitado de usuarios conectados por medio de computadoras alrededor de todo el mundo, entonces parecería natural que muchos de los elementos que conforman esa sociedad estén tomando formando de bits o de bytes. Con el comercio electrónico, llegan los mercaderes electrónicos, los instructores conectados que proveen de educación en línea, doctores que tienen sus citas con sus pacientes en sus oficinas en línea. Y no debería de sorprendernos que también hay criminales cibernéticos cometiendo delitos cibernéticos o crímenes cibernéticos.

El Internet es una gran congregación de corporaciones, individuos, gobiernos, instituciones de educación y todo tipo de organizaciones, que han acordado en principio un set estandarizado de protocolos de comunicación, lo que hace que este servicio se convierta en una vía de comunicación abierta a todos. En

la Superautopista de la Información no hay policías, ni patrullas que estén vigilando con un pistola de radar o deteniendo a aquellos que se ven sospechosos para registrarlos y que no traigan armas. En este medio existe una gran diferencia con las reglas o normas que existen en cualquier calle de cualquier ciudad, de todos los países del mundo y desafortunadamente en el espacio cibernético habita gente sin rostro y sin nombre, todo es virtual.

Haciendo una comparación con la vida real, los crímenes y los criminales vienen en todas las versiones que puede haber en Internet. El FBI tiene una dependencia especial para la prevención y detección de estos crímenes, la National Computer Crime Squad.

Delito Informático:

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

Tipos de Delitos Informáticos:

Infiltración en las Redes Computacionales:

Con la utilización de herramientas de software instaladas en una computadora en cualquier parte del mundo, los hackers pueden irrumpir en cualquier computadora, para robar información, plantar algún virus computacional o los llamados caballos de troya, o simplemente para hacer la travesura de cambiar los nombres de usuarios y claves de acceso (user names & passwords). Este acto esta considerado como ilegal por el Gobierno Federal de los Estados Unidos de Norte América, pero su detección e identificación son muy difíciles. Respecto a esto delito se puede clasificar o castigar de acuerdo a la magnitud del daño ocasionado, si hablamos de algo como cambiar el password de algún usuario, no se le puede castigar de la misma manera que aquel que roba información confidencial o planta algún virus que daña todo un sistema, en ningún momento se debe tratar de defender al "criminal" pero si hay que tener el criterio suficiente para saber medir el daño y en base a eso dar un castigo justo.

Infracción de los derechos de autor:

La interpretación de los conceptos de copia, distribución, cesión y comunicación pública de los programas de ordenador utilizando la red provoca diferencias de criterio a nivel jurisprudencial. No existe una opinión uniforme sobre la responsabilidad del propietario de un servicio on-line o de un sysop respecto a las copias ilegales introducidas en el sistema. El recurso de los propietarios de sistemas on-line y BBS ha sido incluir una advertencia o una cláusula contractual que los exonera de responsabilidad frente a un "upload" de un programa o fichero que infrinja los derechos de autor de terceros.

Infracción del copyright de bases de datos:

No existe una protección uniforme de las bases de datos en los países que tienen acceso a Internet. El sistema de protección más habitual es el contractual, el propietario del sistema permite que los usuarios hagan "downloads" de los ficheros contenidos en el sistema, pero prohibe el replicado de la base de datos o la copia masiva de información.

Interceptación de e-mail :

En este caso se propone una ampliación de los preceptos que castigan la violación de correspondencia, y la interceptación de telecomunicaciones, de forma que la lectura de un mensaje electrónico ajeno revista la misma gravedad.

Estafas electrónicas:

La proliferación de las compras telemáticas permite que aumenten también los casos de estafa. Se trataría en este caso de una dinámica comisiva que cumpliría todos los requisitos del delito de estafa, ya que además del engaño existiría un engaño a la persona que compra. No obstante seguiría existiendo una laguna legal en aquellos países cuya legislación no prevea los casos en los que la operación se hace engañando al ordenador.

Piratas informáticos o hackers:

Este tipo de delincuente aprovecha la falta de rigor de las medidas de seguridad para obtener acceso o puede descubrir deficiencias en las medidas vigentes de seguridad o en los procedimientos del sistema. A menudo, los piratas informáticos se hacen pasar por usuarios legítimos del sistema; esto suele suceder con frecuencia en los sistemas en los que los usuarios pueden emplear contraseñas comunes o contraseñas de mantenimiento que están en el propio sistema, el acceso se efectúa a menudo desde un lugar exterior, situado en la red de telecomunicaciones, recurriendo a uno de los diversos medios que se mencionan a continuación.

Bomba lógica o cronológica:

Este tipo de delito exige conocimientos especializados ya que requiere la programación de la destrucción o modificación de datos en un momento dado del futuro. Por el contrario de los virus, las bombas lógicas son difíciles de detectar antes de que exploten; por eso, de todos los dispositivos informáticos criminales, las bombas lógicas son las que poseen el máximo potencial de daño. Su detonación puede programarse para que cause el máximo de daño y para que tenga lugar mucho tiempo después de que se haya marchado el delincuente. La bomba lógica puede utilizarse también como instrumento de extorsión y se puede pedir un rescate a cambio de dar a conocer el lugar en donde se halla la bomba.

Espionaje:

Se han dado casos de acceso no autorizado a sistemas informáticos gubernamentales e interceptación de correo electrónico del servicio secreto, entre otros actos que podrían ser calificados de espionaje si el destinatario final de esa información fuese un gobierno u organización extranjera. Entre los casos más famosos podemos citar el acceso al sistema informático del Pentágono y la divulgación a través de Internet de los mensajes remitidos por el servicio secreto norteamericano durante la crisis nuclear en Corea del Norte en 1994, respecto a campos de pruebas de misiles. Aunque no parece que en este caso haya existido en realidad un acto de espionaje, se ha evidenciado una vez más la vulnerabilidad de los sistemas de seguridad gubernamentales.

Espionaje Industrial:

Grandes corporaciones como el Gobierno siempre están tratando de espiar al enemigo y los sistemas en red han facilitado esta tarea, como los hackers a sueldo que toman información de los nuevos productos, estrategias de mercadotecnia sin dejar rastro alguno del robo. No sólo es difícil rastrear a los criminales, sino también el condenarlos ya que no hay ninguna ley escrita que este pensada con una mente de robo electrónico. Lo que se supone que mejoraría el desempeño de una empresa ahora se ha vuelto un problema, al correr el riesgo de que la información llegue a ser robada, no importa cuando sistemas de seguridad se puedan desarrollar, no hay que olvidar que a fin de cuentas estos sistemas son diseñados por hombres, por seres humanos, y siempre habrá alguna mente superior a la de su creador que logre violar o encontrar el punto débil de dichos sistemas.

Gusanos:

Se fabrican de forma análoga al virus con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse. En términos médicos podría decirse que un gusano es un tumor benigno, mientras que el virus es un tumor maligno. Ahora bien, las consecuencias del ataque de un gusano pueden ser tan graves como las del ataque de un virus: por ejemplo, un programa gusano que subsiguientemente se destruirá puede dar instrucciones a un sistema informático de un banco para que transfiera continuamente dinero a una cuenta ilícita.

Virus:

Son una serie de claves programáticas que pueden adherirse a los programas legítimos y propagarse a otros programas informáticos. Un virus puede ingresar en un sistema por conducto de una pieza legítima de soporte lógico que ha quedado infectada.

Fraude efectuado por manipulación informática:

Delito que aprovecha las repeticiones automáticas de los procesos de cómputo. Es una técnica especializada que se denomina "técnica del salchichón" en la que "rodajas muy finas" apenas perceptibles, de transacciones financieras, se van sacando repetidamente de una cuenta y se transfieren a otra.

Manipulación de los datos de salida:

Delito que se efectúa fijando un objetivo al funcionamiento del sistema informático. El ejemplo más común es el fraude de que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos. Tradicionalmente esos fraudes se hacían a base de tarjetas bancarias robadas, sin embargo, en la actualidad se usan ampliamente equipo y programas de computadora especializados para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito.

La manipulación de programas:

Este delito consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas. Un método común utilizado por las personas que tienen conocimientos especializados en programación informática es el denominado Caballo de Troya, que consiste en insertar instrucciones de computadora de forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal. En este tipo de delitos el delincuente debe tener conocimientos técnicos concretos de informática.

Manipulación de los datos de entrada:

Este tipo de fraude informático es conocido también como sustracción de datos, representa el delito informático más común ya que es fácil de cometer y difícil de descubrir. Este delito no requiere de conocimientos técnicos de informática y puede realizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos en la fase de adquisición de los mismos.

Piratería de Software:

De acuerdo con la U.S. Software Publisher´s Association, aproximadamente $7.5 billones del Software Americano pudiera ser copiado o distribuido ilegalmente cada año alrededor del mundo. Estas copias funcionan de igual manera que la original y pueden ser conseguidas a menor precio, la piratería es fácil y sólo las grandes organizaciones son capturadas, sin embargo el Pirata sabe que no durara mucho tiempo en la cárcel ya que estas están llenas de personas que han cometido crímenes más serios. La Piratería no sólo daña al productor en

sus ganancias, también lo hace con el usuario ya que cuando se realiza este tipo de compra no se tiene ninguna garantía del buen

Pornografía Infantil:

Este es un crimen que está claro que es ilegal, ya sea en Internet o fuera de él. Algunos operativos han logrado detener a los delincuentes, pero todavía hay manera de obtener imágenes de niños con poca ropa o en diferentes actos sexuales. En materia legal, la gente que usa o provee de pornografía infantil, enfrentan los mismos cargos, ya sea que la fotografía este digitalizada o en un pedazo de papel fotográfico. En los juicios de los usuarios de ese material que fueron arrestados recientemente por el FBI, retarán la validez de las leyes, en cuanto se apliquen a los servicios en línea.

Bombardeo de Correo Electrónico (e-mail bombings):

Las computadoras pueden ser programadas para que hagan casi todo, y de esta manera el Internet se ha visto invadido por el "terrorismo" en el formato de Bombardeo de Correo Electrónico . Programando la computadora para que mande e-mail´s repetidamente a una dirección en específico, el criminal puede inundar el recipiente del usuario y potencialmente apagar sistemas completos. Esto puede ser o no ser ilegal, pero ciertamente es destructivo. También hay e-mail´s como el PenPal Greetings que a la hora de seleccionarlo para leer su contenido se despliega un tipo de virus que borra todo el disco duro de la computadora, además es enviado automáticamente a todos los usuarios que han mandado e-mail´s a esa cuenta, siguiendo el mismo procedimiento de destrucción.

Passwords Sniffers:

Son programas que rastrean el nombre y clave de los usuarios de la red, en el momento en que ellos ingresan, poniendo en juego la seguridad. El que instale un programa de este tipo puede tomar la identidad del usuario y conectarse, logrando tener accesos a documentos restringidos. Las leyes no tienen alguna forma de consignar o procesar a las personas que toman la identidad de otras en línea, pero podrían ser procesadas como hackers que no tienen acceso autorizado y que utilizan estos programas.

Spoofing:

Lo podríamos traducir como engañar, burlar; es el acto de disfrazar una computadora para que parezca otra desde el punto de vista electrónico, con el objeto de obtener acceso a un sistema que por lo regular esta restringido. Legalmente puede ser tratado como los Password Sniffers . Este crimen se cometió recientemente, para sacar información almacenada en la computadora de un "experto en seguridad" Tsutomu Shimomura.

Fraude con Tarjeta de Crédito:

Según el Servicio Secreto de los Estados Unidos, la mitad de un billón de dólares son perdidos anualmente por usuarios con tarjetas de crédito y llamadas de tarjetas robadas a bases de datos en línea. Esto ha triado como consecuencia el que se integren mejores y más fuertes sistemas de seguridad.

La Ley Federal de Derechos de Autor y el Código Penal Federal en materia de fuero común proveen cierta protección sobre los programas de computación, las bases de datos y las infracciones derivadas sobre su uso ilícito esta ley entró en vigor el 24 de marzo de 1997, pero aún existen varios elementos que deben contemplarse sobre la problemática de los derechos de autor en nuestro país, donde unos de los principales es la complejidad de su tipificación, ya que resulta bastante difícil abarcar todas las posibilidades que se presentan dentro de un programa computacional, este es un problema que se presenta al momento de querer crear una regulación que proteja los programas de computo, ya que resulta prácticamente imposible crear un programa de cómputo sin tomar como base otro, siempre es necesario tener la posibilidad de poder tomar parte de un código para la generación de otro, pero de aquí que se aproveche esta situación para hacer uso indebido del código original

Se presentó una iniciativa de Decreto de Reforma al Código Penal para el Distrito Federal en materia de Fuero Federal, proponiendo la adición de un título Vigésimo Sexto denominado "De los delitos en materia de derechos de autor", donde, se consideró conveniente la inclusión de la materia en el ordenamiento materialmente punitivo, lo que por un lado habría de traducirse en un factor de impacto superior para inhibir las conductas delictivas y por otro en un instrumento más adecuado para la procuración y la administración de justicia, al poderse disponer en la investigación de los delitos y en su resolución, del instrumento general que orienta ambas funciones públicas.

Esta Ley regula todo lo relativo a la protección de los programas de computación, a las bases de datos y a los derechos autorales relacionados con ambos. Se define lo que es un programa de computación, su protección, sus derechos patrimoniales, de arrendamiento, casos en los que el usuario podrá realizar copias del programa que autorice el autor del mismo, las facultades de autorizar o prohibir la reproducción, la autorización del acceso a la información de carácter privado relativa a las personas contenida en las bases de datos, la publicación, reproducción, divulgación, comunicación pública y transmisión de dicha información, establece las infracciones y sanciones que en materia de derecho de autor deben ser aplicadas cuando ocurren ilícitos relacionados con los citados programas y las bases de datos, etcétera.

Encontramos dos artículos donde se regula lo referente a los programas de cómputo:

El artículo 102, regula la protección de los programas de computación y señala además que los programas de cómputo que tengan por objeto causar efectos nocivos a otros programas o equipos, lógicamente no serán protegidos.

El artículo 231, sanciona el comercio de programas de dispositivos o sistemas cuya finalidad sea desactivar dispositivos electrónicos de protección de un programa de cómputo.

En el artículo 215 se contempla la sanción al uso de programas de virus.

Si se incluyeran sanciones a la fabricación de programas de virus en el Código Penal lleva implícito el reconocimiento de un delito informático debe tenerse presente que los delitos a regular en este título son en materia de derecho de autor, en el que el bien jurídico a tutelar es la propiedad intelectual, lo que limita su aplicación debido a que en los delitos informáticos el bien jurídico a tutelar serían por ejemplo el de la intimidad, patrimonio, etcétera.

En el artículo 104 se menciona la facultad del titular de los derechos de autor sobre un programa de computación o sobre una base de datos, de conservar aún después de la venta de ejemplares de los mismos el derecho de autorizar o prohibir el arrendamiento de dichos programas.

El artículo 231, en sus fracciones II y VII contemplan dentro de las infracciones de comercio el "producir, fabricar, almacenar, distribuir, transportar o

comercializar copias ilícitas de obras protegidas por esta Ley y usar, reproducir o explotar una reserva de derechos protegida o un programa de cómputo sin el consentimiento del titular", la redacción de estas fracciones tratan de evitar la llamada piratería de programas en el área del comercio, permite la regulación administrativa de este tipo de conducta, como una posibilidad de agotar la vía administrativa antes de acudir a la penal, al igual que las infracciones contempladas para los programas de virus.

Por otro lado la regulación de esta conducta se encuentra reforzada por la remisión que hace la Ley de Derecho de Autor en su artículo 215, donde se sanciona al que incurra en este tipo de delitos. Sin embargo, la regulación existente no ha llegado a contemplar el delito informático como tal, sino que se ha concretado a la protección de los derechos autorales y de propiedad industrial, principalmente.

El Artículo 109, se refiere a la protección de las bases de datos personales, lo que reviste gran importancia debido a la manipulación indiscriminada que individuos deshonestos pueden hacer con esta información.

La protección a bases de datos es necesaria en virtud de que la información contenida en ellas, puede contener datos de carácter sensible, como son los de las creencias religiosas o la filiación política. Adicionalmente pueden ser susceptibles de chantaje, los clientes de determinadas instituciones de créditos que posean grandes sumas de dinero, en fin, la regulación de la protección de la intimidad personal es un aspecto de suma importancia que se encuentra regulado en este artículo.

El artículo 208, que el Instituto Nacional del Derecho de Autor es la autoridad administrativa en materia de derechos de autor y derechos conexos, quien tiene entre otras funciones, proteger y fomentar el derecho de autor además de que está facultado para realizar investigaciones respecto de presuntas infracciones administrativas e imponer las sanciones correspondientes.

Existen diferentes organismos que han decidido enfrentarse la problemática de los delitos informáticos a fin de que contribuyan al desarrollo de este trabajo:

Tratado de Libre Comercio de América del Norte (TLC), es un instrumento internacional firmado por el Gobierno de México, de los Estados Unidos y Canadá en 1993, contiene un apartado sobre propiedad intelectual,

donde se contemplan los derechos de autor, patentes, otros derechos de propiedad intelectual y procedimientos de ejecución.

En términos generales, puede decirse que en ese apartado se establecen como parte de las obligaciones de los Estados signatarios en el área que se comenta que deberán protegerse los programas de cómputo como obras literarias y las bases de datos como compilaciones, además de que deberán conceder derechos de renta para los programas de cómputo.

Otro aspecto importante s que se contempló la defensa de los derechos de propiedad intelectual en el artículo 1714, a fin de que su derecho interno contenga procedimientos de defensa de los derechos de propiedad intelectual que permitan la adopción de medidas eficaces contra cualquier acto que infrinja los derechos de propiedad intelectual comprendidos en el capítulo específico del tratado.

En el artículo 1717 cabe destacar los procedimientos y sanciones penales donde se expresa y contempla la figura de piratería de derechos de autor a escala comercial, podemos encontrar también diversos nexos, donde destaca el titulado "Defensa de la propiedad intelectual", que estableció que México haría su mayor esfuerzo por cumplir tan pronto como fuera posible con las obligaciones del artículo 1718 relativo a la defensa de los derechos de propiedad intelectual en la frontera, haciéndolo en un plazo que no excedería a tres años a partir de la fecha de la firma del TLC.

Asimismo, debe mencionarse que en el artículo 1711, relativo a los secretos industriales y de negocios sobre la provisión de medios legales para impedir que estos secretos, sean revelados, adquiridos o usados sin el consentimiento de la persona que legalmente tenga bajo su control la información.

También se contemplan los requisitos para la protección de los secretos industriales y de negocios y una de ellas es que éstos consten en medios electrónicos o magnéticos.

El comercio menciona ciertas restricciones sobre los derechos de la propiedad intelectual, donde cabe mencionar que el Gobierno de México es parte de este acuerdo que se celebró en el marco de la Ronda Uruguay del Acuerdo General de Aranceles Aduaneros y Comercio (GATT) manteniendo su vigencia hasta nuestros días.

Cabe destacar que en este acuerdo el artículo 10, en lo relativo a los programas de ordenador y compilaciones de datos, se establece que este tipo de programas, ya sean fuente u objeto, serán protegidos como obras literarias de conformidad con el Convenio de Berna de 1971 para la Protección de Obras Literarias y Artísticas, y que las compilaciones de datos posibles de ser legibles serán protegidos como creaciones de carácter intelectual.

Además, en el artículo 41, se incluye que los miembros del acuerdo velarán porque en su respectiva legislación nacional se establezcan procedimientos de observancia de los derechos de propiedad intelectual.

En el artículo 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 artículo 69 marca lo relativo a la cooperación internacional, donde se establece el intercambio de información y la cooperación entre las autoridades de aduanas en lo que se refiere al comercio de mercancías de marca de fábrica o de comercio falsificadas y mercancías pirata que lesionan el derecho de autor.

Estos instrumentos internacionales abarca las conductas ilícitas relacionadas con las computadoras en el marco del derecho de autor.

En el año de 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 computacionales., las posibles implicaciones económicas de la delincuencia informática, su carácter internacional y, a veces, incluso transnacional y el peligro de que la diferente protección jurídico - penal nacional pudiera perjudicar el flujo internacional de información, condujeron en consecuencia a un intercambio de opiniones y de propuestas de solución. Sobre la base de las posturas y de las deliberaciones surgió un análisis y valoración incomparativista de los derechos nacionales aplicables así como de las propuestas de reforma. Se concluyó en una lista de las acciones que pudieran ser consideradas por los Estados, por regla general, como merecedoras de pena.

De esta forma, la OCDE en 1986 publicó un informe titulado Delitos de Informática, que incluye un análisis de la normativa jurídica, en 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, como lo es el fraude y la falsificación informática, la alteración de datos y programas de computadora, sabotaje informático, acceso no autorizado, interceptación no autorizada y la reproducción no autorizada de un programa de computadora protegido.

La mayoría de los miembros de la Comisión Política de Información, Computadores y Comunicaciones recomendó también que se instituyesen protecciones penales contra otros usos indebidos, espionaje informático, utilización no autorizada de una computadora, utilización no autorizada de un programa de computadora protegido, incluido el robo de secretos comerciales y el acceso o empleo no autorizado de sistemas de computadoras.

Con objeto de que se finalizara la preparación del informe de la OCDE, el Consejo de Europa inició su propio estudio sobre el tema a fin de elaborar directrices que ayudaran a los sectores legislativos a determinar qué tipo de conducta debía prohibirse en la legislación penal y la forma en que debía conseguirse ese objetivo, teniendo debidamente en cuenta el conflicto de intereses entre las libertades civiles y la necesidad de protección.

La lista mínima preparada por la OCDE se amplió considerablemente, añadiéndose a ella otros tipos de abuso que se estimaba merecían la aplicación de la legislación penal. El Comité, Especial de Expertos sobre Delitos relacionados con el empleo de las computadoras, del Comité Europeo para los problemas de la Delincuencia, examinó esas cuestiones y se ocupó también de otras, como la protección de la esfera personal, las víctimas, las posibilidades de prevención, asuntos de procedimiento como la investigación y confiscación internacional de bancos de datos y la cooperación internacional en la investigación y represión del delito informático.

Una vez desarrollado todo este proceso de elaboración de las normas a nivel continental, el Consejo de Europa aprobó la recomendación R(89)9 sobre delitos informáticos, en la que se "recomienda a los gobiernos de los Estados miembros que tengan en cuenta cuando revisen su legislación o preparen una nueva, el informe sobre la delincuencia relacionada con las computadoras .... y en particular las directrices para los legisladores nacionales". Esta recomendación fue adoptada por el Comité de Ministros del Consejo de Europa el 13 de septiembre de 1989.

Se incluyó una lista mínima, que refleja el consenso general del Comité, acerca de determinados casos de uso indebido de computadoras y que deben incluirse en el derecho penal, así como una lista facultativa que describe los actos que ya han sido tipificados como delitos en algunos Estados pero respecto de los cuales no se ha llegado todavía a un consenso internacional en favor de su tipificación.

Por otro lado en 1992, la OCDE 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 el mismo año.

En este contexto, consideramos que si bien este tipo de organismos gubernamentales ha pretendido desarrollar normas que regulen la materia de delitos informáticos, es resultado de las características propias de los países que los integran, quienes, comparados con México u otras partes del mundo, tienen un mayor grado de informatización y han enfrentado de forma concreta las consecuencias de ese tipo de delitos.

Por otra parte, a nivel de organizaciones intergubernamentales de carácter universal, debe destacarse que en el seno de la Organización de las Naciones Unidas (ONU), en el marco del Octavo Congreso sobre Prevención del Delito y Justicia Penal, celebrado en 1990 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, donde la injerencia transnacional en los sistemas de proceso de datos de otros países, había traído la atención de todo el mundo. Por lo que el problema principal hasta este momento era la reproducción y la difusión no autorizada de programas informáticos y el uso indebido de los cajeros automáticos, no se habían difundido otras formas de delitos informáticos, por lo que era necesario adoptar medidas preventivas para evitar su aumento, pero se supuso que habría un gran número de casos de delitos informáticos no registrados, por lo que , en vista de que los delitos informáticos eran un fenómeno nuevo, y debido a la ausencia de medidas que pudieran contrarrestarlos, se consideró que el uso deshonesto de las computadoras podría tener consecuencias desastrosas. A este respecto, el Congreso recomendó que se establecieran normas y directrices sobre la seguridad de las computadoras a fin de ayudar a la comunidad internacional a hacer frente a estas formas de delincuencia.

Partiendo del estudio comparativo de las medidas que se han adoptado a nivel internacional para atender esta problemática, deben señalarse los problemas que enfrenta la cooperación internacional en la esfera del delito informático y el derecho penal, a saber: la falta de consenso sobre lo que son los delitos informáticos, falta de definición jurídica de la conducta delictiva, falta de conocimientos técnicos por parte de quienes hacen cumplir la ley, dificultades de carácter procesal, falta de armonización para investigaciones nacionales de delitos informáticos. Adicionalmente, la ausencia de la equiparación de estos delitos en los tratados. internacionales de extradición.

Teniendo presente esa situación, se considera que es indispensable resaltar que las soluciones puramente nacionales serán insuficientes frente a la dimensión internacional que caracteriza este problema, en consecuencia, es necesario que para solucionar los problemas derivados del incremento del uso de la informática, se desarrolle un régimen jurídico internacional donde se establezcan las normas que garanticen su compatibilidad y aplicación adecuada. Durante la elaboración de dicho régimen, se deberán considerar los diferentes niveles de desarrollo tecnológico que caracterizan a los miembros de la comunidad internacional.

También es importante mencionarse que la Asociación Internacional de Derecho Penal durante un coloquio celebrado en Wurzburgo en 1992, adoptó diversas recomendaciones respecto a los delitos informáticos. Estas recomendaciones contemplaban que en la medida en que el derecho penal tradicional 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. Además, las nuevas disposiciones deberán ser precisas, claras y con la finalidad de evitar una excesiva tipificación deberá tenerse en cuenta hasta que punto el derecho penal se extiende a esferas afines con un criterio importante para ello como es el de limitar la responsabilidad penal con objeto de que éstos queden circunscritos primordialmente a los actos deliberados.

Tomando en cuenta la importancia de la informática y las posibilidades delictivas que puede entrañar el adelanto tecnológico, se recomendó que los Estados consideraran de conformidad con sus tradiciones jurídicas y su cultura y con referencia a la aplicabilidad de su legislación vigente, poniendo gran interés especialmente en la alteración de datos de computadora y el espionaje informático; así como que por lo que se refiere al delito de acceso no autorizado precisar más al respecto en virtud de los adelantos de la tecnología de la información y de la evolución del concepto de delincuencia.

Otro aspecto importante es el tráfico con contraseñas informáticas obtenidas por medios inapropiados, la distribución de virus o de programas similares deben ser considerados también como susceptibles de penalización.

En los Estados Unidos de Norteamérica existe el Estatuto de Fraude y Abuso Computacional ; el cual contiene diversos artículos o capítulos en los menciona los casos en los que se comenten diferentes delitos informáticos. Podemos tomar por ejemplo el 1030. Relacionado con el Fraude y actividades que tengan que ver con computadoras, en donde se mencionan las características de los ilícitos:

Tener el conocimiento de los passwords de acceso a una computadora sin autorización o rebasando los límites a los que está autorizado, con el objeto de obtener información que este determinada por el Gobierno Federal de los Estados Unidos como razones de Defensa Nacional o Relaciones Exteriores; además de la Información sobre Energía Atómica, tal como se contempla en la Atomic Energy Act de 1954, con el objeto de lastimar al país o proporcionarla a otro país para aventajar a los Estados Unidos.

Violar el acceso a una computadora intencionalmente con el objeto de obtener información sobre los estados financieros de alguna institución.

Hacer uso de cualquier equipo de computo que pertenezca a alguna agencia de los Estados Unidos, sin autorización, o accesar a esa computadora que es exclusivamente para el uso del Gobierno, y que esto dañe las operaciones realizadas por el gobierno en ese sistema.

Accesar sin autorización a una computadora de interés federal, con el objetivo de cometer algún fraude y obtener alguna ganancia de tipo económica.

Para todas estas actividades existe una sanción que van desde multas, hasta el cumplimiento de una sentencia en una penitenciaria o centro de rehabilitación; lo que se trata de hacer es de tener algo con que defender a los usuarios de los medios informáticos; llegando de esta manera a fijar las multas o indemnizaciones de acuerdo al daño, perdida, ocasionado además de una sentencia justa para aquellos que la gravedad de sus actos lo ameriten.

El problema más común al que se enfrentan las autoridades es al supuesto desconocimiento de las consecuencias de los actos de las personas o a la comparación con los delitos de la vida cotidiana como por ejemplo alguien puede

decir "Técnicamente no he cometido un crimen, lo único que hice fue destruir información, no robe nada"[1] es por esto que las leyes aún no han podido llegar a la acertada aplicación de las mismas con una fuerza suficiente.

Los usuarios de las redes deben de tener mucho cuidado de no cometer ilícitos y sobre todo de no ser víctima de los mismos. Diferentes instituciones, sistemas legales de todas partes están estudiando ampliamente la forma de lidiar con los criminales cibernéticos y sobre todo de tipificar los delitos que se cometen para poder hacer más fuerte la sanción a los criminales informáticos. Un buen consejo sería que se hiciera una legislación de tipo Mundial para este tipo de delitos ya que en la actualidad, los delitos y los delincuentes son tratados de diferentes maneras en las distintas jurisdicciones.

Bibliografía:

http://tiny.uasnet.mx/prof/cln/der/silvia/tipos.htm
http://tiny.uasnet.mx/prof/cln/der/silvia/tipos.htm
http://www.aui.es/biblio/libros/mi96/p1.htm
http://www.eff,org/pub/EFF/Legislation/Bills_new/s314.bill
http://www.phantom.com/~slowdog/
http://www.phantom.com/~slowdog/
http://www.panix.com/vtw/exon/exon.html
http://www.derecho.unam.mx/ligas.html
http://www.derecho.unam.mx/ligas.html
http://www.uaq.mx/academ/invest/virus.html
http://www.uaq.mx/academ/invest/virus.html
http://www.sc.ehu.es/docen/lsi.html
http://www.arrakis.es/~neromar/derecho/dchos/informat.html
http://www.arrakis.es/~neromar/derecho/dchos/informat.html
http://www.nlpnet.com/buddies/arlekin/virus.htm
http://www.ontrack.com/busqueda.html
http://www.digitalcentury.com/encyclo/update/crime.html
http://www.digitalcentury.com/encyclo/update/crime.html
http://www.aracnet.com/~gtr/archive/investigate.html
http://www.aracnet.com/~gtr/archive/investigate.html
http://www.smu.edu/~jwinn/digitech/dtlcrime.html
http://www.smu.edu/~jwinn/digitech/dtlcrime.html

[1] Recombinant Culture: Crime in the Digital Network, Curtis E.A. Karnow; Copyright © 1994 Curtis Karnow

http://www.cspr.org/cspr/privacy/crime/crime.html
http://www.cspr.org/cspr/privacy/crime/crime.html

"Derecho Informático", Tellez Valdes, Julio.. 2ª. ed. México. Ed. Mc Graw Hill 1996.

"Leyes y Negocios en Internet "Hance Olivier.. México. De. Mc Graw Hill Sociedad Internet. México. 1996.