DELITOS INFORMÁTICOS DELITOS ELECTRÓNICOS
Autora: Lic. Maria de Lourdes Delgado Granados

PRÓLOGO

El manejo de la Internet ha provocado que todos los ámbitos, jurídico, cultural, social, etcétera, se hayan visto afectados; el derecho que por años, cuando menos en México, había tenido pocos cambios se ha convulsionado igual que otros ámbitos.

En México, la cultura informática en la administración pública ha tenido un desarrollo impresionante, a nivel gubernamental se ha propiciado el manejo de los medios electrónicos, tanto es así que el sistema de contratación gubernamental se efectúa, a través del programa denominado "compranet", que resultó ganador y obtuvo un premio a nivel internacional equiparable al premio Nóbel, en el año de 1999, entregado en Estocolmo, dado que es un programa de vanguardia y que ha propiciado diversos acuerdos con otros países, a efecto de instalarlo. Otro programa el trámite de gestiones administrativas se lleva a cabo por medio de "tramitanet"; la declaración de bienes de los servidores públicos se hace por medio de Internet, utilizando el programa "declaranet".

Todo lo anterior es novedoso, importante y trascendente, pero para centrarnos en el tema que ahora nos inquieta e interesa, o sea, la materia jurídica, específicamente los delitos en que se incurra con la aplicación de las nuevas tecnologías, se ha de tomar en cuenta si tenemos en México legislación aplicable a los nuevos adelantos de la ciencia, y qué ilícitos en relación con los procedimientos electrónicos se han presentado.

Para concluir lo anterior, es menester tomar en cuenta algunas definiciones que han tratado de perfilar el delito electrónico y el de los actores en su comisión.

Antecedentes

La revolución informática ha originado que no exista área que no se encuentre afectada por el fenómeno. Ante dicha situación, varios países han tomado las previsiones jurídicas que impone el caso y México no es la excepción.

Así es como se ha desarrollado lo que en la actualidad se conoce como derecho informático.

Derecho Informático (Concepto)

Se puede definir al derecho informático como el conjunto de normas jurídicas tendientes a regular la propiedad, uso y abusos de los equipos de cómputo y de los datos que se transmiten en forma electromagnética.

El derecho informático en nuestro país, todavía es incipiente.

Delitos Informáticos

Los **delitos informáticos,** llamados también delitos cibernéticos, delitos electrónicos, delitos relacionados con las computadoras, delincuencia relacionada con el ordenador, computer related crimes, etc. se han definido por la **Organización para la Cooperación Económica y el Desarrollo,** como:

"Cualquier conducta ilegal, no ética o no autorizada que involucra el procesamiento automatizado de datos y/o la transmisión de datos".

En esta definición podemos encontrar elementos de valoración ética que son trascendentes para el derecho penal.

En nuestro país ya existe legislación que regula las novedosas relaciones y realidades que se vinculan con la computación.

La problemática de los delitos informáticos requiere un estudio especial en nuestro país con vistas a determinar la medida en que la legislación penal (códigos penales y leyes especiales) deba prever la incidencia en los citados ilícitos.

Una de las peculiaridades de este tipo de delitos es que desafortunadamente no conllevan una problemática local; la existencia de redes internacionales como Intemet abren la posibilidad de transgresiones a nivel mundial y con gran impunidad.

August Bequal, en su intervención "Computer Related Crimes" en el **Council of Europe, señala algunos de** los riesgos que se corren en este caso:

"Si prosigue el desorden político mundial, las redes de cómputo globales y los sistemas de telecomunicaciones atraerán seguramente la ira de terroristas y facinerosos." (Ya hemos observado la realidad)

"Las guerras del mañana serán ganadas o perdidas en nuestros centros de cómputo, más que en los campos de batalla."

Concepto

El delito informático implica actividades criminales que en un primer momento los países han tratado de encuadrar en figuras típicas de carácter tradicional, tales como robos o hurtos, fraudes, falsificaciones, perjuicios, estafa, sabotaje, etcétera. 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.

En materia internacional se considera que no existe una definición 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.

"Cualquier acción ilegal en que una computadora es herramienta u objeto del delito".

"Cualquier incidente asociado con tecnología de cómputo en que una víctima sufre o puede sufrir pérdida y una intromisión intencional, propiciando o pudiendo propiciar una ganancia".

"Delito electrónico ", en un **sentido amplio** es cualquier conducta 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 lícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel, ya sea como método, medio o fin".

Por otra parte, debe mencionarse que se han formulado diferentes denominaciones para indicar las conductas ilícitas en las que se usa la computadora, tales como delitos informáticos", delitos electrónicos, delitos relacionados con las computadoras", "crímenes por computadora". "delincuencia relacionada con el ordenador".

Es evidente que el objeto de todos los estudios, es la regulación penal de aquellas actitudes antijurídicas estimadas graves, como último recurso para evitar su impunidad.

El concepto de abuso informático incluye una diversidad de ofensas, tanto penales como administrativas; algunas de éstas constituyen delitos que ya se castigan en diversas legislaciones; sin embargo, quedan conductas que aún no encuentran tipificadas en legislaciones penales.

¿Por qué tipificar? Sería la pregunta. si se coincide con el planteamiento de que los delitos patrimoniales tradicionales seguirán dañando uno de los bienes jurídicos más importantes de la esfera individual, después de la vida, seguridad corporal, la propiedad, respeto a la intimidad, etc., como lo es el derecho a comunicación, no se puede contradecir la pertinencia de incluir dentro del catálogo penal aquellas conductas que son cometidas con o por medio de computadoras, de las que resultan pérdidas económicas graves.

Sobre el delito informático, Diego Castro Fernández, en su artículo "El delito informático" publicado en la Revista Jurídica núm. 41 en San José, Costa Rica, **comenta la existencia de dos tipos de elementos en estos actos:**

Es **elemento objetivo,** la acción, tanto la que afecta los componentes de la computadora (hardware y software), como medio o instrumento para perpetrar el delito, así como la consumación de un acto ilícito autónomo como es el uso indebido y sin autorización de una computadora ("robo de tiempos").

Se menciona también el **elemento subjetivo** de la conducta, consistente en el dolo, culpa o preterintención en la comisión del delito.

Elementos Activo y Pasivo

En forma enunciativa, no limitativa y todavía sin atender a las necesidades de la realidad nacional en esta área, se presentará una descripción de los **sujetos activos y pasivos** de este tipo de delitos.

En este extremo es pertinente hacer una precisión. Tradicionalmente se ha considerado que este tipo de delitos encuadra dentro de los llamados "delitos de cuello blanco" debido a que se requiere que el sujeto activo tenga un conocimiento especializado en informática.

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 de 1943.

Efectivamente, este conocido criminólogo señala un sin número de conductas que considera como "delitos de cuello blanco", aun 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, 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".

Retomando la idea, se puede ubicar como **sujeto activo** de un delito cibernético a un lego en la materia o a un empleado de un área no informática que tenga un mínimo conocimiento de computación. Por no hablar del problema que se plantea con los llamados "niños genio" que son capaces no sólo de dominar sistemas electrónicos básicos, sino que pueden incluso intervenir exitosamente en operaciones de alto grado de dificultad técnica, acarreando más problemas al tambaleante concepto de la impunidad para el
caso de que algunos de estos menores logre cometer estragos importantes, a través de los medios computacionales que maneje.

Clasificación de los Delitos

En México se reconoce la copia ilegal de programas de cómputo como un delito en la Ley de Derechos de Autor, así como la copia ilegal de topografías (como diseños industriales) en la Ley de Propiedad Industrial.

En el extranjero se han reconocido como modalidades de delitos informáticos, los siguientes: Manipulaciones, el espionaje, el sabotaje y el hurto de tiempo.
Donn B. Parker señala el modus operandi de la delincuencia informática, en un listado que seguramente se incrementará en la medida en que la tecnología avance y los delincuentes encuentren formas cada vez más eficaces de cometer daños, tales son:

La instrucción de datos engañosos (data didling), caballo de Troya (trojan horse), redondeo de cuentas (salami techniques), uso indebido de programas (superzapping), puertas con trampa (trap doors), bombas lógicas (logic bombs), ataques asincrónicos (asynchronic attacks), obtención de información residual (scavenging), filtración de datos (data leakage), acceso a áreas no autorizadas (piggy backing and impersonation wiretapping), y simulación y modelo de delitos convencionales (simulation and modeling).

La conducta seguida, a través de las formas antes señaladas, tiene que ver con la carencia de una ética tecnológica, originada por la rapidez con que la misma tecnología gana espacios en las sociedades, y el estupor con que se enfrenta la problemática, que incita paradójicamente en esta novedosa forma de procesamiento de información, es decir, las computadoras.

Tipos de Delitos Informáticos

La propia complejidad de la red es una dificultad para la detección y corrección de los múltiples y variados problemas de seguridad que van apareciendo. Es importante recalcar que es importante para la protección de los sistemas, la

atención y vigilancia continua y sistemática por parte de los gestores de la red. Se recoge una lista exhaustiva de problemas detectados, extraída del libro: "Firewalls and Internet Security. Repelling the Willy Hacker(...)".

Lista de peligros más comunes en sistemas conectados a internet

1.- De todos los problemas, el mayor son los fallos en el sistema de passwords.

2.- Los sistemas basados en la autenticación de las direcciones se pueden atacar usando números consecutivos.

3.- Es fácil interceptar paquetes UDI?.

4.- Los paquetes ICMP pueden interrumpir todas las comunicaciones entre dos nodos (Muchos más).

Tipos de delitos informáticos reconocidos por Naciones Unidas:

Delito. Características.

Fraudes cometidos mediante manipulación de computadoras.

Manipulación de los datos. Este tipo de fraude informático 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.

La manipulación de programas es difícil de descubrir y a menudo pasa inadvertida debido a que el delincuente debe tener conocimientos técnicos concretos de informática. 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.

Manipulación de los datos de salida. 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.

Fraude efectuado por manipulación informática 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.

Falsificaciones informáticas, como objeto cuando se alteran datos de los documentos almacenados en forma computarizada.

Como instrumentos. Las computadoras pueden utilizarse también para efectuar falsificaciones de documentos de uso comercial. Cuando empezó a disponerse de

fotocopiadoras computarizadas, en color, a base de rayos láser, surgió una nueva generación de falsificaciones o alteraciones fraudulentas. Estas fotocopiadoras pueden hacer copias de alta resolución, pueden modificar documentos e incluso pueden crear documentos falsos, sin tener que recurrir a un original, y los documentos que producen son de tal calidad que sólo un experto puede diferenciarlos de los documentos auténticos.

Daños o modificaciones de programas o datos computarizados.

Sabotaje informático. Es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema. Las técnicas que permiten cometer sabotajes informáticos son:

Virus. Es 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, así como utilizando el método del Caballo de Troya.

Gusanos. Se fabrica 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 ¡lícita.

Bomba lógica o cronológica. Exige conocimientos especializados, ya que requiere la programación de la destrucción o modificación de datos, en un

momento dado del futuro. Ahora bien, al revés de los virus o los gusanos, 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.

Acceso no autorizado a servicios y sistemas informáticos.

Por **motivos diversos,** desde la simple curiosidad, como en el caso de muchos piratas informáticos (hackers) hasta el sabotaje o espionaje informático.

Piratas informáticos o hackers. 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. El delincuente puede aprovechar 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.

Reproducción no autorizada de programas informáticos de protección legal. Esta puede entrañar una pérdida económica sustancial para los propietarios legítimos. Algunas jurisdicciones han tipificado como delito esta clase de actividad y la han sometido a sanciones penales. El problema ha alcanzado dimensiones transnacionales con el tráfico de esas reproducciones no autorizadas, a través de las redes de telecomunicaciones modernas.

[mdelgadog@mail.scjn.gob.mx]