Capítulo 7
Delito Informático

En este capítulo se revisan las generalidades
del delitos informático,
su clasificación y los tipos de delitos informáticos,
en general aspectos laborales de la Informática.

Introducción

El manejo de la información dentro de las organizaciones es esencial para su operación, esta información es resultado del esfuerzo de la institución para recabarla, clasificarla, almacenarla y procesarla, esta situación convierte a la información en un recurso invaluable ya que la pérdida de la misma, su modificación, fuga y su posible caída en manos de la competencia o de enemigos puede ocasionar daños invaluables, pérdida de mercado o de recursos capitalizables, prestigio y aún más llevar a una empresa a la quiebra o a la pérdida de credibilidad.

Lo anterior hace necesario tipificar, normar y legislar al delito informático en las organizaciones. Los fraudes electrónicos, el robo de información, la cada vez mayor participación de individuos sin profesionalismo y ética que no administran de manera prudente y segura la información y que además generan códigos nocivos que afecta por igual a los sistemas de información como al ambientes de cómputo, instalaciones y redes de comunicación, provocando con esto daño a los datos.

El material aquí presentado fundamentalmente se centra en los actos en Informática que se definen por sí mismos como actividades perjudiciales y riesgosas.

II.7.1 Generalidades

Fuente: Téllez Valdés, Julio. "Derecho Informático".
2a. ed. México. Ed. McGraw Hill 1996.

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 hurto, 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 el ámbito internacional se considera que no existe una definición propia del delito informático, sin embargo muchos han sido los esfuerzos de expertos que se han ocupado del tema, y aún cuando no existe una definición con carácter universal, se han formulado conceptos funcionales atendiendo a realidades nacionales concretas.

Cabe destacar que no es labor fácil dar un concepto sobre delitos informáticos, en razón de que su misma denominación alude a una situación muy especial, ya que para hablar de "delitos" en el sentido de acciones típicas, es decir tipificadas o contempladas en textos jurídicos penales, se requiere que la expresión "delitos informáticos" esté consignada en los códigos penales, lo cual en nuestro país, al igual que en otros muchos no ha sido objeto de tipificación aún".

Para Carlos Sarzana [50], 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, como mero símbolo".

Lidia Callegari [51] define al delito informático como "aquel que se da con la ayuda de la informática o de técnicas anexas".

Rafael Fernández Calvo[52] 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 un 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 [53] 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".

[50] Sarzana, Carlo. "Criminalità e tecnologia" en Computers Crime. Rassagna Penitenziaria e Criminologia. Nos. 1-2 Año 1. Roma, Italia.
[51] Callegari, Lidia. "Delitos informáticos y legislación" en Revista de la Facultad de Derecho y Ciencias Políticas de la Universidad Pontificia Bolivariana. Medellín, Colombia. No. 70 julio-agosto-septiembre. 1985.
[52] Fernández Calvo, Rafael. "El tratamiento de llamado "delito informático" en el proyecto de ley Orgánico del Código Penal: reflexiones y propuestas de la CLI (Comisión de libertades e informática) en Informática y Derecho.
[53] Lima de la Luz, María. "Delitos Electrónicos" en Criminalia. México. Academia Mexicana de Ciencias Penales. Ed. Porrúa. No. 1-6. Año L. Enero-Junio 1984.

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" en sus formas típica y atípica[54], "delitos electrónicos", "delitos relacionados con las computadoras", "crímenes por computadora", "delincuencia relacionada con el ordenador".

En este orden de ideas, se entenderán como *"*delitos informáticos" *todas aquellas conductas ilícitas susceptibles de ser sancionadas por el derecho penal, que hacen uso indebido de cualquier medio informático.*

Lógicamente este concepto no abarca las infracciones administrativas que constituyen la generalidad de las conductas ilícitas presentes en México debido a que la legislación se refiere a derecho de autor y propiedad intelectual.

Fuente: Del Pont K., Luis Marco y Nadelsticher Mitrania, Abraham, "Delitos de cuello blanco y reacción social", Instituto Nacional de Ciencias Penales. México. 1981.

Sujeto activo

Las personas que cometen los "Delitos informáticos" son aquellas que poseen ciertas características que no presentan el denominador común de los delincuentes, esto es, los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación labora 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[55].

Sin embargo, tendiendo 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*"[56]

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.

[54] El delito informático en forma típica se entiende por "la conducta antijurídica y culpable en que se tienen a las computadoras como instrumento o medio" y por la atípica por las "actitudes ilícitas en que se tienen a las computadoras como objetivo o fin".

[55] Aniyar de Castro, Lolita. El delito de cuello blanco en América Latina: una investigación necesaria. ILANUD AL DÍA. Año 3 No.8 Agosto 1980. San José, Costa Rica.

[56] Término introducido por primera vez por el criminológico norteamericano Edwin Sutherland en el año de 1943.

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 casualmente por el desconocimiento del "*modus operandi*" de los sujetos activos.

Dado lo anterior, ha sido imposible conocer la verdadera magnitud de los "*delitos informáticos*", ya que la mayor parte de los delitos no son descubiertos.

II.7.2 Clasificación del delito informático

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

Los delitos informáticos se clasifican sobre la base de dos criterios:

- Como instrumento o medio
- 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.

- Falsificación de documentos vía computarizada (Tarjetas de crédito, cheques, etc.).
- Variación de los activos y pasivos en la situación contable de las empresas.
- Planeación o simulación de delitos convencionales (robo, homicidio, fraudes, etc.).
- Lectura, sustracción o copiado de información confidencial.
- Modificación de datos, tanto en la entrada como en la salida.
- Aprovechamiento indebido o violación de un código para penetrar a un sistema, introduciendo instrucciones inapropiadas.
- Variación en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta bancaria, apócrifa.
- Uso no autorizado de programas de cómputo
- Alteración en el funcionamiento de los sistemas
- Acceso a áreas informatizadas en forma no autorizada
- Intervención en las líneas de comunicación de datos.
- Introducción de instrucciones que provocan "interrupciones" en la lógica interna de los programas.

Como fin y objetivo

Conductas criminógenas dirigidas contra la entidad física del objeto o máquina electrónica o su material con objeto de dañarla.

◊ Programación de instrucciones que producen
◊ un bloqueo total al sistema.
◊ Destrucción de programas por cualquier método.
◊ Daño a la memoria.
◊ Atentado físico contra la maquina o sus accesorios
◊ (discos, cintas, terminales, etc.).
◊ Sabotaje político - terrorismo en que se destruye o surge un apoderamiento de los centros neurálgicos computarizados.
◊ Secuestro de soportes magnéticos en los que figure información valiosa con fines de chantaje, pago de rescate, etc.

II.7.3 Tipos de delitos informáticos (reconocidos por Naciones Unidas)

Fraudes informáticos

- Manipulación de los datos de entrada.- 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 muy 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 tiene 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 partir de tarjetas bancarias robadas, sin embargo, en la actualidad se usan ampliamente el 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 de 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 basándose en 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 en 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.

- 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 donde se halla la bomba.

- Acceso no autorizado a servicios y sistemas informáticos..- Es el acceso no autorizado a sistemas informáticos por motivos diversos: desde la simple curiosidad, como en el caso de muchos piratas informáticos (hackers) hasta el sabotaje o espionaje informático. 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.- La reproducción no autorizada de programas informáticos 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 moderna.

Medidas preventivas

Cabe sugerir que para poder combatir este tipo de ilícitos es necesario un control y tener en consideración medidas preventivas, a través de diversas formas de carácter administrativo, normativo y técnico, de entre las principales tenemos.

- ✓ Elaboración de un examen psicométrico previo al ingreso al área de sistemas en las empresas.

- ✓ Introducción de cláusulas especiales en los contratos de trabajo con el personal informático que por el tipo de labores a realizar así lo requiera.

- ✓ Establecimiento de un código ético de carácter interno en las empresas.

- ✓ Adoptar estrictas medidas en el acceso y control de las áreas informáticas de trabajo.

- ✓ Capacitación adecuada del personal informático a efecto de evitar actitudes negligentes.

- ✓ Identificación y, en su caso, segregación del personal informático descontento.

- ✓ Rotación en el uso de claves de acceso al sistema (passwords).

Por otra parte, en cuanto concierne al control correctivo, esté podrá darse en la medida en que se introduzcan un conjunto de disposiciones jurídicas específicas en los códigos penales sustantivos, ya que en caso de considerar este tipo de ilícitos como figuras análogas ya existentes, corre el riesgo de alterar flagrantemente al principio de legalidad de las penas.

Fuente: Asociación latinoamericana de profesionales en seguridad informática, A. C.
"Memorias del Foro de Consulta sobre Derecho e Informática", Guadalajara, Jal. Septiembre de 1996

Tipificación de delitos

- Espionaje: el robo de información por cualquier medio informático ya sean magnéticos, impresos o por consultas no autorizadas a esos medios, así como la intercepción de las comunicaciones o medios de transmisión de la información.

- Sabotaje: se puede dar con la destrucción u ocultamiento de la información, con la inhabilitación de los sistemas operativos o de los equipos de cómputo o comunicaciones, así como la interferencia de las comunicaciones.

- Fraude: se da con la desviación de los recursos capitalizables o activos propiedad de otra persona física o moral u organismo público, haciendo uso de prácticas desleales dentro del sistema informático o con un ataque externo a los medios de seguridad informáticos. La inexistencia de los citados medios no atenúa el delito.

- Negligencia: se da debido a la falta del establecimiento de procedimientos seguros, así como de la falta de preparación y aún de ética de los operadores, administradores y usuarios de los medios informáticos. Esa falta de preparación de los recursos humanos no exime de responsabilidades a los particulares por los daños ocasionados.

- Abuso de confianza: se da cuando una de las partes incumple un contrato de confidencialidad y proporciona información a un tercero. También se da cuando un patrón o administrador recaba información de unos de sus empleados y hace uso de esa información sin consentimiento del interesado en beneficio propio o de un tercero.

- Violación de los derechos de autor: se da con la copia no autorizada por escrito del autor de un programa de cómputo con la intención diferente del respaldo, como puede ser la comercialización, explotación o la modificación.

- Atentado contra la seguridad nacional: son todas las actividades citadas anteriormente las cuales tengan una intención comprobable de socavar la soberanía de la nación, la paz y seguridad pública y el estado de derecho en general.

- Divulgación de datos privados: se da cuando una persona física o moral, hace pública alguna información privada que tenga sobre otra sin su autorización, con la intención de poner en evidencia la moral y el honor de la misma. La falta de comprobación de la intención no exime de responsabilidades a quien hace la divulgación.

Valor probatorio del documento electrónico en procesos administrativos y judiciales.

- Confiabilidad: es la propiedad del documento de ser disponible para su lectura en cualquier momento y lugar con los medios apropiados. Con la certeza de no haber sido modificado por manos ajenas al autor o autoridad que lo recaba.

- Integridad: es la propiedad del documento de ser completo en sus partes con la finalidad proporcionar toda la información disponible y sin ambigüedad.

- Veracidad: es la propiedad del documento de contener información apegada a la realidad.

II.7.4 Aspectos laborales de la informática

Fuente: Téllez Valdés Julio, "Derecho informático", UNAM, México, 1991

Los aspectos laborales de la informática, "van a ser todo el conjunto de implicaciones de orden normativo-laboral provocados por el uso de la informática" [57].

Dentro de las principales implicaciones podemos citar.

- Movilización de puestos y desempleo.
- Condiciones de trabajo.
  - Jornadas de trabajo.
  - Vacaciones y días de descanso.
  - Salario.
- Derechos y obligaciones de los patrones y trabajadores.
- Categoría contractual.
- Riesgos de trabajo.

Valor probatorio de los soportes informáticas.

Las pruebas son hechos, surgen de la realidad extra-jurídica, del orden natural de las cosas. Las pruebas no son una creación del derecho. Su existencia y valor se toma de la realidad extra-jurídica preconstruidas como fuentes (documento, testigo, cosa litigiosa, etc.) y constituidas como medios (actuaciones judiciales, como por ejemplo la declaración de un testigo).

De entre los principales medios de prueba se tienen:

- Confesional: es una declaración de parte que contiene el reconocimiento de un hecho de consecuencias jurídicas desfavorables para el confesante.

- Documental: también llamadas literal, es la que se hace por medio de documentos, en la forma previamente establecida en las leyes procesales.

- Pericial: se deriva de la apreciación de un hecho por parte de un observador con preparación especial, obtenida por el estudio de la materia a que se refiere, o simplemente por la experiencia personal.

[57] Téllez Valdés Julio, "Contratos informáticos", UNAM, México, 1991

- Testimonial: dada por los testigos como aquellas personas que comunican al juez el conocimiento que posee de determinado hecho (o hechos), cuyo esclarecimiento interesa para la decisión de un proceso.

- Inspección judicial: consiste en un examen directo por el juez de la cosa mueble o inmueble sobre que recae para formar su convicción sobre el estado o situación en que se encuentra en el momento en que la realiza pueda ser fuera o en el juzgado.

- Fama pública: estado de opinión sobre un hecho que se prueba mediante el testimonio de personas que la ley considera hábiles para este efecto.

- Presunciones: aquellas operaciones lógicas mediante las cuales, partiendo de un hecho conocido, se llega a la aceptación como existente de otro desconocido o incierto.

Delitos de daño por cualquier medio.

Cuando por cualquier medio se causan daños, destrucción o deterioro de cosas ajenas, o de cosa propia, en perjuicio de tercero, se aplicaran las reglas del robo simple, un claro ejemplo de delito de daño por cualquier medio en materia de informática, lo tenemos en: Virus de computadora, es decir, un conjunto de instrucciones que se propagan así mismas a través de la computadora, para realizar acciones destructivas.

Cabe hacer la aclaración que el virus en la mayoría de los casos es generado por obtener una copia "pirata" de un programa, por lo que se considera en ese momento como un delito por cualquier medio al equipo o medio informático, que se utilice a parte de la obtención de dicha copia y si el fabricante del programa genero un virus para proteger sus programas de dichas copias, en ese momento no es considerado como delito para el fabricante.

El tipo penal anteriormente descrito, corresponde al delito de daños por cualquier medio.

La hipótesis que se desprenda del tipo legal de daños por cualquier medio, descrita en el código penal [58], son:

- Una conducta, que puede ser dolosa o imprudencial, es decir, puede cometerla tanto alguien a propósito, como un operador cualquiera al introducir programas no autorizados que no han pasado el debido proceso de revisión y desinfección. Se aconseja en tal caso prescindir del software (serie de instrucciones que realizan una tarea y son intangibles) pirata.

[58] Artículo 399 del código penal

- El resultado consistente en: la destrucción, daños o deterioro de una cosa; esa cosa puede ser ajena, o propia. Tomando en consideración que se habla de la destrucción o el deterioro tanto de informaciones, como de programas.

- Con perjuicio para tercero: Este elemento es imprescindible para que se configure el delito. No es difícil de probar, si el afectado es, por ejemplo, el cliente o consumidor, los compradores mayoristas, los proveedores, el licenciante de un programa de computación por el cual se pagarán regalías periódicas, etc.

En orden a la conducta, el delito de daños por cualquier medio puede ser doloso, en cuyo caso, "se implicarán las reglas del robo simple" para la imposición de sanciones. O bien puede ser una conducta imprudencial, en cuyo caso la punibilidad (castigo), la determinará el juez conforme a los criterios del código penal [59].

Bibliografía de este capítulo:

1. Téllez Valdés, Julio. "Derecho Informático", 2a. ed. México. Ed. Mc Graw Hill 1996.
2. Del Pont K., Luis Marco y Nadelsticher Mitrania, Abraham, "Delitos de cuello blanco y reacción social", Instituto Nacional de Ciencias Penales. México. 1981.
3. Asociación latinoamericana de profesionales en seguridad informática, A. C. "Memorias del Foro de Consulta sobre Derecho e Informática", Guadalajara, Jal. Septiembre de 1996

[59] Artículo 60 del código penal