Delitos Cibernéticos

JULIO TÉLLEZ VALDÉS

Profesor Universidad Nacional Autónoma de México

Orígenes

Así como la computadora se presenta como una herramienta muy favorable para la sociedad, también se puede constituir en un instrumento u objeto en la comisión de verdaderos actos ilícitos.

Concepto típico y atípico.

Dependiendo de su tipificación o no tenemos que, los delitos cibernéticos son "actitudes ilícitas en que se tiene a la Cibernética como instrumento o fin" (concepto atípico) o las "conductas típicas, antijurídicas y culpables en que se tiene a la Cibernética como instrumento o fin" (concepto típico) .

Principales Características

a) son conductas criminógenas de cuello blanco (white collar crimes), en tanto que sólo determinado número de personas con ciertos conocimientos (en este caso técnicos) pueden llegar a cometerlas.

b) son acciones ocupacionales en cuanto que muchas veces se realizan cuando el sujeto se halla trabajando.

c) son acciones de oportunidad en cuanto que se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico.

d) provocan serias pérdidas económicas, ya que casi siempre producen "beneficios" de más de cinco cifras a aquellos que los realizan.

e) ofrecen facilidades de tiempo y espacio, ya que en milésimas de segundo y sin una necesaria presencia física pueden llegar a cometerse.

f) son muchos los casos y pocas las denuncias y todo ello debido a la misma falta de contemplación por parte del derecho.

g) son sumamente sofisticados y relativamente frecuentes en el ámbito militar.

h) presentan grandes dificultades para su comprobación, esto, por su mismo carácter técnico.

i) en su mayoría son imprudenciales y no necesariamente intencionales.

j) ofrecen facilidades para su comisión a los menores de edad.

h) tienden a proliferar cada vez más, por lo que requieren una urgente regulación.

l) por el momento siguen siendo ilícitos manifiestamente impunes ante la ley.

Clasificación

1. Como instrumento o medio

En esta categoría tenemos a las conductas criminógenas que se valen de las computadoras como método, medio o símbolo en la comisión del ilícito, por ejemplo:

a) falsificación de documentos vía computarizada (tarjetas de crédito, cheques, etcétera).

b) variación de los activos y pasivos en la situación contable de las empresas.

c) planeación o simulación de delitos convencionales (robo, homicidio, fraude, etcétera).

d) "robo" de tiempo de computadora.

e) lectura, sustracción o copiado de información confidencial.

f) modificación de datos tanto en la entrada como en la salida

h) aprovechamiento indebido o violación de un código para penetrar a un sistema introduciendo instrucciones inapropiadas (esto es lo que se conoce en el medio como el método del "caballo de troya").

i)variación en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta bancaria apócrifa, método conocido como la técnica de salami".

j)uso no autorizado de programas de cómputo.

k)introducción de instrucciones que provocan "interrupciones" en la lógica interna de los programas, a fin de obtener beneficios.

l)alteración en el funcionamiento de los sistemas.
obtención de información residual impresa en papel o cinta magnética luego de la ejecución de trabajos.

n)acceso a áreas informatizadas en forma no autorizada.

o)intervención en las líneas de comunicación de datos o teleproceso.

2. Como fin u objetivo

En esta categoría encuadramos a las conductas criminógenas que van dirigidas en contra de la computadora, accesorios o programas como entidad física. algunos ejemplos son los siguientes:

a) programación de instrucciones que producen un bloqueo total al sistema.

b) destrucción de programas por cualquier método.

c) daño a la memoria.

d) atentado físico contra la máquina o sus accesorios (discos, cintas, terminales, etcétera) .

e) sabotaje político o terrorismo en que se destruya o surja un apoderamiento de los centros neurálgicos computarizados.

f) secuestro de soportes magnéticos en los que figure información valiosa con fines de chantaje, pago de rescate, etcétera) .

Formas de control preventivo y correctivo

-- 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, éste podrá darse en la medida en que se introduzcan un conjunto de disposiciones jurídicas especificas en los códigos penales sustantivos, ya que en caso de considerar este tipo de ilícitos como figuras análogas ya existentes se corre el riesgo de alterar flagrantemente el principio de legalidad de las penas.

Cabe hacer mención que una adecuada legislación al respecto traería consigo efectos no sólo correctivos sino eventualmente preventivos, de tal forma que se reducirían en buen número este tipo de acciones que tanto daño causan a los intereses individuales y sociales.

Situación en México

Nuestro actual código penal sustantivo de 1931, no se ajusta de ninguna manera a este tipo de manifestaciones tecnológicas, además de que en él se atiende a un criterio preponderantemente subjetivo, y tal vez sería conveniente considerar la necesidad de contemplar o dar cabida a criterios más propiamente objetivos, esto en atención a la gran importancia que adquieren cada vez con más fuerza este tipo de instrumentos como lo son las computadoras.

Debido a la importancia que ha venido revistiendo la falta de regulación expresa que sanciones aquellas conductas tendientes a utilizar a los sistemas informáticos como medio o fin comisivo de diversos ilícitos, es que se exponen las diversas problemáticas y situaciones en la que nos encontramos inmersos, mismas que deben ser solucionadas a la brevedad, a efecto de que se pueda continuar el normal desarrollo social-informático, pero esta vez ya protegido de todos o la mayoría de posibles actitudes negativas.

Luz María del Pozo nos habla de un Delito Electrónico, refiriéndose a este como "Aquel que se comete con el uso de computadoras o cualquier otro medio electrónico, como pueden ser las telecomunicaciones."

De igual forma el Antonio Aveleyra nos comenta que el Delito Cibernético, son aquellas "Conductas antisociales cometidas, teniendo como objeto del delito o como medio de comisión a las tecnologías y a los sistemas de información; las conductas combatir pueden entonces ser muy amplias y revestir muy variadas formas".

Dentro de las diversas Instituciones el manejo de la información es el resultado de todo un procedimiento, convirtiendo a ésta en un recurso invaluable, ocasionando su perdida o alteración que pueda hacerse un mal uso de ésta, provocando con ello serios daños a dicha institución o incluso a terceras personas.

Los fraudes electrónicos, el robo de información, la generación cada vez más frecuente de códigos nocivos que afectan a sistemas de cómputo y redes de comunicación es un daño a los datos, mismos que deben de ser tipificados como delitos.

Su tipificación se ha buscado, entre otras, a través de las siguientes figuras jurídicas

- espionaje
- sabotaje
- fraude
- negligencia
- abuso de confianza
- violación de los derechos de autor
- atentado contra la seguridad nacional
- divulgación de datos privados

En México, ha falta de una regulación particularizada se han recurrido a los siguientes tipos contemplados en el Código Penal :

- Ataques a la vías generales de comunicación. (art.167 fracs. II, VI y IX.)
- Violación de correspondencia (art.173)
- Revelación de secretos (art. 210)

- Fraude genérico (art. 387 fracs. II, III, VII, X, XVI, XIX, 388)

- Abuso de confianza (art. 382)

- Robo (art. 367)

- Extorsión (art. 309)

- Espionaje (art.127)

- Sabotaje (art.140)

- Daños por cualquier medio (art.399)

Algunas características adicionales de estos delitos son las siguientes :

- Crecimiento masivo de los medios informáticos a nivel mundial.

- En todos lados algunas personas se han dedicado a buscar los modos de burlar los sistemas de acceso de las computadoras y redes computacionales, y desgraciadamente cada vez pueden lograr hacer más daño.

- Debido al incipiente sistema de seguridad en el acceso de las computadoras, continuamente algunos usuarios se crean cuentas con derechos excesivos sobre alguna área de la red, llegando a realizar actividades susceptibles de conocerse como delitos, como sería el caso del apoderamiento de archivos, su manipulación, su utilización, su producción no autorizada por el autor o el titular del derecho, o finalmente su destrucción, proponiendo que se podría equiparar al daño en propiedad ajena.

- Es necesario que los administradores de las redes de cómputo sean ingenieros de sistemas computacionales, además de contar con los conocimientos certificados para la adecuada operación del sistema de red.

- Análisis del problema.

La falta de preparación de la personas a cargo de las redes computacionales, las hace muy vulnerables a la introducción de personas ajenas a éstas.

La responsabilidad de los administradores de una red de cómputo, puede ser de dos tipos: culpables o no culpables.

- Propuesta.

Se propone crear el tipo penal de responsabilidad de las administradores de redes de cómputo, contando con las siguientes bases:

a) Que contando con los conocimientos debidos, para prevenir la comisión de un ilícito por un tercero no actúen.

b) Que actúen de manera negligente ante el descubrimiento del irrumpimiento de un hacker, o ante la existencia de cuentas con derechos excesivos sobre determinados directorios de la red.

c) Que perpetúen ellos mismos el ilícito consistente en el apoderamiento, modificación, utilización o destrucción no autorizada por el autor o el titular del derecho sobre el archivo.

Cuando se comete el Delito Cibernético, afecta a gran número de entidades como son:

- los seres humanos
- los gobiernos de las naciones
- las corporaciones
- las integridades económicas, de personas, de empresas y naciones.
- los países en su soberanía.
- las industrias (con el espionaje industrial)

En términos generales se necesita una regulación jurídica en los siguientes campos:

- prevención

- caracterización del delito cibernético

- determinación técnica del grado delictuoso

- fijación de las responsabilidades

- determinación de negligencia

- establecer restitución propicia al causar daños.

- fijar indemnización por daños.

- capacitación obligatoria de los ejecutivos en un centro de cómputo.

- establecer la obligación de reportar los delitos electrónicos.

Para Aveleyra, las principales conductas antisociales que se deben tomar en cuenta para formular los nuevos tipos penales, son las siguientes:

I.- Constituyendo conductas antisociales preponderadamente contra los bienes patrimoniales:

1.Conductas contra la economía, tal como el abuso fraudulento en las instalaciones de procesamiento de datos;

2.Adquisición no autorizada de información;

3.Daño a programas;

4.Robo de tiempo;

5.Fraudes a la contabilidad;

6.Apoderamiento de claves;

7.Substracción de efectivo;

8.Dañar las computadoras y líneas telemáticas;

9.Beneficios indebidos por el uso inadecuado de bancos de datos;

10. Interferencia con los negocios de otro;

11. Piratería de programación o su adquisición ilegal;

12. Fraude por medios informáticos;

13. Robo de dinero o de servicios, o de información confidencial, o de programas, o de tiempo.

14. Apoderamiento no autorizado de información, disco o programas.

II.- Constituyendo conductas antisociales preponderadamente contrarias a los bienes informacionales o a los derechos de las personas, tenemos:

1.Acceso no autorizado a la información e intercepción de informaciones y comunicaciones;

2.Negar el acceso o uso si autorizados;

3.Negar la información autorizada;

4.Abuso y daño de información e introducción de información falsa a la computadora.

5.Adquisición ilegal de información;

6.Espionaje informático;

7.Violación del derecho a la autodeterminación informacional;

8.Violación de la privacidad.