UNIVERSIDAD VIRTUAL HISPÁNICA DE MÉXICO

LICENCIATURA EN DERECHO

<<LOS SABERES RESPECTO DE LOS DELITOS CIBERNETICOS>>

TESIS

PARA OBTAR

LA LICENCIATRURA EN DERECHO

PRESENTA LA ALUMNA:

LETICIA CONCHA LÓPEZ

DIRECTORA DE TESIS: MTRA. MARI CARMEN CONCHA LÓPEZ

2013.

Agradezco a dios por las bendiciones y permitirme lograr mis objetivos

A mis padres, hermana y sobrina por su apoyo incondicional.

A mi asesora la Mtra. Maricarmen Concha López por el apoyo incondicional para el desarrollo y culminación de esta tesis.

CAPITULO I

ASPECTOS BASICOS

INDICE **PÁGINAS**

AGRADECIMIENTOS

1.1 Anomia de la prevención del delito cibernético 1

1.2 Definición de cibercriminalidad 1

1.3 La web 3

1.4 El internet 4

1.4.1 Ética en el manejo del internet 5

1.5 La cibercriminalidad en el derecho penal 6

1.6 La cibercriminalidad en el ámbito internacional 8

1.6.1 Tratados internacionales 9

1.6.2 Las Naciones Unidas y los delitos cibernéticos 11

1.7 Valores que son afectados por la cibercriminalidad 12

1.8 Nuevas formas de criminalidad 13

1.8.1 Factores que incrementan la cibercriminalidad 15

1.9 Características de los delitos cibernéticos 15

CAPITULO II

SUJETOS DE LA DELINCUENCIA CIBERNETICA

2.1 Generalidades 17

2.2 Sujetos activos 17

2.2.1 Características de los sujetos activos 19

2.3 Clases de delincuentes cibernéticos 19

2.4 Tipos de delincuentes cibernéticos 20

2.4.1 Piratas informáticos 20

2.4.2 Phreaker 21

2.4.3 Delincuente informático 21

2.5 Sujetos adictos a la tecnología 22

2.6 Sujetos pasivos 23

2.7 Vulnerabilidad de los sujetos pasivos 25

2.8 Bien jurídico protegido 25

2.8.1 Bienes jurídicos protegidos en el delito cibernético 26

CAPITULO III:

CONCIDERACION TECNICA Y METODO PARA EVITAR LOS DELITOS CIBERNETICOS

3.1 Consideraciones 28

3.2 Catalogo de los delitos cibernéticos 29

3.2.1 El delito informático 30

3.2.2 Crímenes específicos 31

3.2.3 Fraude 32

3.2.4 Pishing 32

3.2.5 Hostigamiento 33

3.2.6 Trafico de drogas 34

3.2.7 Terrorismo virtual 34

3.3 Eficacia en la técnica de investigación respecto de los delitos cibernéticos 35

3.4 Reglas para proteger a los afectados con los delitos cibernéticos 35

3.5 Los delitos cibernéticos y la policía 36

3.6 Medios de prueba utilizados en la comprobación de los delitos Cibernéticos 37

3.7 Inmutabilidad de las pruebas para los delitos cibernéticos 38

3.8 Promoción, control y evacuación de los medios de prueba 38

3.9 Cadena de custodia 39

3.10 Impacto de los delitos cibernéticos 39

3.10.1 Impacto a nivel general 39

3.10.2 Impacto a nivel social 40

3.10.3 Impacto en la esfera judicial 40

CAPITULO IV:

CONTROL ADECUADO DE LOS DELITOS CIBERNÉTICOS

4.1 Manejo de los delitos cibernéticos en la averiguación previa 42

4.2 Hecho delictivo 43

4.3 Peritos 44

4.3.1 Perito cibernético 45

4.3.1.1 Deberes profesionales del perito 46

4.3.2 Áreas de intervención de los peritos cibernéticos 49

4.3.3 Con el dictamen pericial 49

4.3.3.1 Estructura del dictamen pericial 49

4.4 Implicaciones de los peritos y sus efectos 50

4.4.4 Función del agente del ministerio publico en los delitos cibernéticos 51

4.5 Recomendaciones para no ser víctima de delitos cibernéticos 52

4.6 Recomendaciones para los padres 52

4.7 Recomendaciones para los niños y adolescentes 53

4.8 Recomendaciones para los docentes 54

4.9 Aplicación de un simulador con tarjeta de adquisición de datos 55

CONCLUSIONES 58

POSFACIO 60

FUENTES DE INFORMACION 61

PRESENTACION

La observación empírica que de manera directa aprecie sobre el buen o mal uso del Internet, así como la actuación irregular de los Agentes del ministerio publico, Policías y Peritos en el ciberespacio, fue la causa que impulso esta investigación, ante el esquema de la globalización y la dependencia de las tecnologías que propician ambientes agresivos y lesivos afectando la economía, paz social y la estabilidad del gobierno.

En la presente tesis se confronta el objeto de estudio en las dimensiones epistémicas de los niveles del conocimiento, teórico, normativo y practico describiendo el fenómeno sociológico jurídico y se vierten recomendaciones a efecto de evitar conductas lesivas para las personas.

Por lo tanto el contenido temático se ocupa en el primer capítulo de aspectos básicos normativos, en el capitulo segundo se aborda el tema de los sujetos que intervienen en los delitos cibernéticos. En el capítulo tercero se mencionan pasos metódicos para evitar la comisión de delitos cibernéticos y en el cuarto capítulo se hace alusión a recomendaciones a efecto de evitar conductas cibernéticas lesivas de la esfera jurídica de las personas. Por último, vierto conjeturas respecto de la importancia de evitar la comisión de delitos cibernéticos. Y desde luego dejo a la crítica y observaciones del lector el saber sistemático, que se debe realizar sobre los delitos cibernéticos.

CAPITULO I

ASPECTOS BASICOS

1.1 Anomia de la prevención del delito cibernético

No existen textos normativos que denoten y expliquen metodológicamente un procedimiento para lograr una correcta seguridad jurídica en la red cibernética. Operativamente se hace alusión a guías básicas para el mismo fin a través de acuerdos establecidos por las procuradurías de los estados, pero no existe normatividad alguna, lo que origina seguridad jurídica en la investigación.

Durkheim estima que anomia es el mal que sufre una sociedad a causa de la ausencia de reglas morales y reglas jurídicas, es decir es la ausencia de la norma. Esta ausencia se debe al desequilibrio económico y al debilitamiento de sus instituciones, que implica un bajo grado de integración social.[1] La anomia es un colapso de gobernabilidad por no poder controlar esta situación emergente de alienación provocando un comportamiento no social. De tal manera, que la anomia en cuanto a la ausencia de legislación respecto a los delitos cibernéticos, provoca el entorpecimiento en el proceso de investigación dificultando, el ejercicio o no de la acción penal, puesto que no se allegan a todos los elementos del delito.

1.2 Definición de cibercriminalidad

Se entiende por cibercriminalidad aquellas acciones que han sido cometidas mediante la utilización de un bien o servicio informático, sin

[1] DURKHEIM, Emili, *"Escritos Selectos, Introducción y selectos de Anthony Gidenns",* Editorial Buenos Aires, Nueva Visión, México D.F. 1993, Pág. 115

dejar a un lado que un sistema informático también es un bien jurídico que recibe protección por parte del ordenamiento jurídico. El desarrollo de las Tecnologías de la Información y las Comunicaciones (TIC) con lo que ello supone: desarrollo del comercio electrónico, globalización de la economía, posibilidad de acceso a diversos recursos, etc., abre una nueva posibilidad de delitos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos.[2]

En la práctica, el término cibercriminalidad engloba tres tipos de actividades delictivas: 1ro. Comprende formas tradicionales de delincuencia, como el fraude o la falsificación, aunque en el contexto cibernético se refiere específicamente a los delitos cometidos mediante las redes de comunicaciones y los sistemas de información electrónicos (redes electrónicas). 2do. Se refiere a la publicación de contenidos ilegales a través de medios de comunicación electrónicos (por ejemplo, imágenes de abuso sexual a menores o incitaciones al odio racial). 3ro. Incluye delitos específicos de las redes electrónicas, por ejemplo los ataques contra los sistemas informáticos, la denegación de servicio y la piratería. Estos ataques también se pueden dirigir contra infraestructuras críticas fundamentales de un país o comunidad y afectar a sistemas de alerta rápida existentes en numerosos ámbitos, con consecuencias potencialmente desastrosas para el conjunto de la sociedad.[3]

[2] GRANDE, Edwin, *"La cibercriminalidad en el presente",* Editorial Esquino, México D.F. 2003, Pág. 15

[3] GUERRERO, MATÉUS, Fernanda, *"Ciberdelincuencia"*, Procuraduría General de la Nación. 2004, Pág. 218

1.3 La web

La concepción de la computadora, se remonta a los años treinta del siglo XIX, época en la que el matemático ingles Charles Babbage intento construir una calculadora llamada maquina analítica se basaba en los mismos principios de los ordenadores modernos, con la diferencia de que los datos codificados, en lugar de pasar a través de compuertas lógicas se introducían a través de un sistema de piñones y ruedas dentadas, Babbage dedico los últimos 37 años de su vida a la construcción de esta máquina pero no logro completarla, fue imposible construir con la precisión suficiente algunas piezas de la máquina. Buena parte de sus ideas fueron retomadas posteriormente por Tim Berners Lee y Mark Andreessen. (Andreesen, 2001)

Al respecto, el autor en cita, señala que (203, 2004): “La web inicio en 1960 para conectar las computadoras de una misma empresa, en 1976 Tim y Mark, encontraron la forma de realizar una computadora atractiva y muy fácil de usar”. Tim escribió un programa para juntarlo todo en su pantalla de computadora y llamo al programa averigüe aquí sobre lo que sea” el programa utilizaba hipertexto para teclear y llegar a nuevas páginas de información. El programa de Tim solo funcionaba en las computadoras que usaban los científicos hasta que hizo público su código.

En Estados Unidos Andreessen lo modifico para que funcionara en las computadoras personales y lo llamo Moisac. Era un buscador que modificaba una pequeña y desconocida red de computadoras en el modo global de intercambiar información. En 1993 solo había 50 servidores al

siguiente año había 10 000 hoy en día existen casi treinta y cinco millones de servidores. Mediante el World Wide Web podemos obtener imágenes, sonidos y palabras de computadoras dispersas por todo el globo terráqueo. No necesitamos saber en donde esta almacenada la información que buscamos: solo hacemos clic para encontrarla.

Cabe mencionar que la computadora ya forma parte de nuestra vida cotidiana y se utiliza para almacenar enormes cantidades de información y procesarla a gran velocidad. Cualquiera que se a su tamaño y complejidad, toda computadora está compuesta por cuatro elementos básicos: el equipo de entrada que suele ser el teclado, la memoria en que se almacena la información, la unidad central de procesamiento que lleva a cabo las instrucciones o comandos, y el equipo de salida, que suele estar formado por el monitor y la impresora. La computadora como un medio de tecnología bastante avanzado y que con el uso adecuado no seremos vulnerados en nuestra esfera jurídica.

1.4 El Internet

Es una red de computadoras conectadas entre sí. Esta red permite el intercambio de información entre diferentes computadoras ubicadas en distintas partes del mundo se utiliza un lenguaje común a todas las máquinas llamado protocolo. El intercambio de información crea un universo virtual formado por información contenida en medios electrónicos de almacenamiento de orden físico, existen diferentes métodos de comunicación como el mail que funciona como un correo tradicional, el ftp que funciona como el sistema de intercambio de libros de la biblioteca, el servicio web que consiste en una "página" en la que se coloca cierto tipo

de información sobre algún tema en particular. El servicio funciona como un tabloide de anuncios o como un sistema de reparto de propaganda, El Internet como vehículo no tan sólo de la información, sino de medios para llevar a cabo actos de comercio como compras, rentas, arrendamientos.[4]

Estos métodos de comunicación han propiciado una revolución en el mundo entero, de ahí que haya sido comparado al tercer movimiento de cambio de la humanidad, por ello se le ha considerado un prodigio para el desarrollo de un gran número de actividades del ser humano, visto de este modo se podría estimar que nada de malo tiene un bien accesible a la humanidad a través de corriente eléctrica y un equipo PC de bajo costo, aunque actualmente hay tantas innovaciones tecnológicas que el Internet corre incluso a través del teléfono celular; sin embargo, el Internet también representa un gran reto y problema, nos referimos a que ha sido utilizado cono vehículo para llevar a cabo conductas delictivas que han propiciado en el menor de los daños intromisión a la privacidad de las comunicaciones, y en otras situaciones han causado graves daños al patrimonio de las personas e incluso también ha dado pauta, a que individuos conformen bandas de delincuencia organizada que por su nivel de tecnificación han llevado a cabo conductas graves, este fenómeno

1.4.1 Ética en el manejo del Internet

Considero que deben existir reglas de etiqueta del comportamiento por parte de los usuarios, como lo afirma Raz, en una sociedad de ángeles es menester crear reglas para que sus intereses no choquen entre sí, luego

[4] CASSOU,RUIZ, Jorge Esteban, "Delitos informáticos en México", Editorial Nueva imagen, 2009, Págs. 11- 19

entonces, ante un sistema de comunicación mundial, que comprende una gran disparidad de cultura, edad, educación, no tan sólo es congruente sino indispensable crear un manual del comportamiento del usuario, manual que no debe limitarse a un estadio nacional, sino a un plano internacional, con la distinción de que no debe encontrarse elevado a la categoría de una norma con todos sus atributos legales, pero que sí debe servir de patrón para una mejor interacción en el Internet, y para desmotivar en principio, conductas reprobables, así como conductas lesivas de la esfera de los individuos.

La regulación del Internet es un enorme reto en razón de su carácter internacional y de la enorme cantidad de sitios que existen de tan variada índole e interés por ejemplo las personas que juegan en casinos virtuales sin ninguna regulación, a la fecha actual se puede decir que el único contenido de Internet prohibido y sancionado en nuestro país es el de la pornografía infantil. Lo anterior de manera somera da una idea de lo grave que resulta carecer de reglas de comportamiento en el Internet; considero que los valores fundamentales de la sociedad, con independencia de la raza, credo, cultura y educación, son necesarios para la interacción en ese mundo virtual, es por ello que los usuarios del Internet deben ser conscientes y actuar de buena fe, expresando los datos que corresponden a su identidad.

1.5 La Cibercriminalidad en el derecho Penal

La cibercriminalidad como consecuencia de una acción u omisión socialmente peligrosa, prohibida por ley bajo la conminación de una sanción penal a la que es considerada delito informático, pues de forma

expresa se manifiesta como la "acción típica, antijurídica y dolosa cometido mediante el uso normal de la informática contra el soporte lógico o software, de un sistema de tratamiento autorizado de la información.[5]

Esta dimensión transgresora y abusiva del empleo de las nuevas tecnologías debe ser enfrentada por el Derecho Penal, como disciplina garante de la convivencia pacífica e instrumento ultimo de control social.[6]

Debido a la naturaleza virtual de los delitos cibernéticos, puede volverse confusa la tipificación de éstos ya que a nivel general, se poseen pocos conocimientos y experiencias en el manejo de ésta área. Desde el punto de vista de la Legislatura es difícil la clasificación de estos actos, por lo que la creación de instrumentos legales puede no tener los resultados esperados, sumado a que la constante innovación tecnológica obliga a un dinamismo en el manejo de las Leyes relacionadas con la informática.

Al igual que en el resto de los delitos existe un **sujeto activo** y otro pasivo, pero en el caso del primero no estamos hablando de delincuentes comunes (a pesar de que nos referimos tanto a las personas naturales como a las personas jurídicas). El hecho de que no sea considerado el sujeto activo delincuente común está determinado por el mecanismo y medio de acción que utilice para llevar producir el daño, quiénes en la

[5] FARINELLA, Flavio, "*Algunas notas sobre el spamming y su regulación*", AR: Revista de Derecho Informático, núm. 094, mayo de 2006, Pág. 15

[6] GRANDE, Edwin, *"La cibercriminalidad en el presente"*, Editorial Esquino, México D.F. 2003, Págs.9-14

mayoría de los supuestos en que se manifiestan y las funciones que desempeñan pueden ser catalogados sujetos especiales.

Al respecto, el autor en cita, señala (18-21, 2003): “El reconocimiento de varias clases de conductas antijurídicas que puede manifestar el sujeto activo, expresadas en el presente capítulo, es preciso para conocer las posibles formas de comisión delictiva y obviamente profundizar en las posibles formas de prevención y detención de estas conductas”.

La falta de cultura informática es un factor crítico en el impacto de los delitos informáticos en la sociedad en general, cada vez se requieren mayores conocimientos en tecnologías de la información, las cuales permitan tener un marco de referencia aceptable para el manejo de dichas situaciones.

1.6 La Cibercriminalidad en el Ámbito Internacional

En el ámbito internacional comenzaron a prevenir los delitos cibernéticos mediante el convenio sobre la Ciberdelincuencia de fecha 23 de noviembre del año 2001, firmado en Budapest, Hungría, en la que estados de Europa propusieron medidas para prevenir actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas, redes y datos informáticos; conscientes de garantizar el debido equilibrio entre los intereses de la acción penal y el respeto de los derechos humanos fundamentales consagrados en el Convenio del Consejo de Europa para la Protección de los Derechos Humanos y de las Libertades Fundamentales (1950), el Pacto Internacional de Derechos Civiles y Políticos de las Naciones Unidas (1966) y otros tratados internacionales

aplicables en materia de derechos humanos, que reafirman el derecho de todos a defender sus opiniones sin interferencia alguna, así como la libertad de expresión, que comprende la autonomía de buscar, obtener y comunicar información e ideas de todo tipo, sin consideración de fronteras, así como el respeto de la intimidad. A este convenio fue invitado México en el año 2007, de él derivó la Campaña Nacional contra el Delito Cibernético en el año 2008 y el 24 de octubre del año 2011 la reforma al Título Noveno del Código Penal Federal, relativa a la Revelación de Secretos y Acceso Ilícito a Sistemas y Equipos de Informática. Al respecto, el autor en cita, señala (21, 2003) “En Argentina, Canadá, Colombia, España, Estados Unidos de América, Reino Unido los delitos cibernéticos reciben el nombre específico de delitos informáticos”.

1.6.1 Tratados Internacionales

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

El GATT, se transformó en lo que hoy conocemos como la Organización Mundial de Comercio (OMC), por consecuencia todos los acuerdos que se suscribieron en el marco del GATT, siguen estando vigentes. Al respecto, el autor en cita, señala (281, 2003): “En el Art. 61 se establece que para los casos de falsificación dolosa de marcas de fábrica o de comercio o de piratería lesiva del derecho de autor a escala comercial se establecerán procedimientos y sanciones penales además de que "Los recursos disponibles comprenderán la pena de prisión y/o la imposición de sanciones pecuniarias suficientemente disuasorias".

Entre los convenios que encontramos y en los cuales se hace alusión a los delitos cibernéticos encontramos:

- El convenio de Berna
- La convención sobre la Propiedad Intelectual de Estocolmo
- La Convención para la Protección y Producción de Fonogramas de 1971.
- La Convención Relativa a la Distribución de Programas y Señales

En 1983 la Organización de Cooperación y Desarrollo Económico (OCDE) inició un estudio de la posibilidad de aplicar y armonizar en el plano internacional las leyes penales, a fin de luchar contra el problema del uso indebido de los programas de computación. Las posibles implicaciones económicas de la delincuencia informática tienen carácter internacional e incluso transnacional, cuyo principal problema es la falta de una legislación unificada que, facilita la comisión de los delitos.[7]

En 1986 la OCDE público un informe titulado Delitos cibernéticos: análisis de la normativa jurídica, donde se reseñaban las normas legislativas vigentes y las propuestas de reforma en diversos Estados miembros y se recomendaba una lista mínima de ejemplos de uso indebido que los países podrían prohibir y sancionar en leyes penales. En 1992 elaboró un conjunto de normas para la seguridad de los sistemas de información, con intención de ofrecer las bases para que los Estados y el sector privado pudieran erigir un marco de seguridad para los sistemas informáticos.

[7] TÉLLEZ VALDÉS, Julio, *"Derecho informático",* 3ª. ed., México, McGraw-Hill, 2004, p. 163.

Al respecto, el autor en cita, señala (171, 2004): “En 1990 la Organización de las Naciones Unidas (ONU) en el Octavo Congreso sobre Prevención del Delito y Justicia Penal, celebrado en La Habana, Cuba, se dijo que la delincuencia relacionada con la informática era consecuencia del mayor empleo del proceso de datos en las economías y burocracias de los distintos países y que por ello se había difundido la comisión de actos delictivos”.

En 1992 La Asociación Internacional de Derecho Penal durante el coloquio celebrado en Wurzburgo, adoptó diversas recomendaciones respecto a los delitos cibernéticos, entre ellas una ampliación en cuanto a los delitos ya existentes.

1.6.2 Las Naciones Unidas y los delitos cibernéticos

Al respecto la ONU público un Manual para la Prevención y Control de Delitos cibernéticos, en el que señala que cuando una conducta delictiva se eleva a la escena internacional, se magnifica las insuficiencias, los delitos cibernéticos constituyen una forma de crimen trasnacional y su combate requiere de una eficaz cooperación concertada. Asimismo la ONU resume de la siguiente manera a los problemas que rodean a la cooperación internacional en el área de los delitos informáticos:

- Falta de acuerdos globales acerca de qué tipo de conductas deben constituir delitos cibernéticos.
- Ausencia de acuerdos globales en la definición de dichas conductas delictivas.

- Falta de especialización en los cuerpos policiacos y otros funcionarios judiciales en el campo de los delitos cibernéticos.
- Falta de armonización entre las diferentes leyes procesales nacionales acerca de la investigación de los delitos cibernéticos.
- Carácter trasnacional de muchos delitos cometidos mediante el uso de las computadoras.
- Ausencia de tratados de extradición, de acuerdos de ayuda mutua y de mecanismos sincronizados que permitan la puesta en vigor de la cooperación internacional. (Angel Montiel Castro, 1997)

1.7 Valores que son afectados por la cibercriminalidad

Terrel Bynum, basándose en Moor, identifica y analiza los impactos de las tecnologías de la información en los valores humanos y sociales y nos dice que los valores afectados son la salud, la riqueza, el trabajo, la libertad, la democracia, el conocimiento, la privacidad, la seguridad o la autorrealización personal. En este concepto se quieren incluir términos, teorías y métodos de disciplinas como la ética aplicada, la sociología de los ordenadores, la evaluación social de las tecnologías o el derecho informático.[8]

La intención es incorporar una conciencia social relacionada con la tecnología informática y también ayudar a los informáticos a utilizar los ordenadores no solo con eficiencia sino con criterios éticos. El objetivo es tomar decisiones sobre temas tecnológicos de manera consistente con la afirmación de los propios valores que uno profesa o con los derechos humanos en general.

[8] TERREL, Bynum, *"Delitos informáticos",* Editorial Parris, 2 Edición, México D.F.2001, Pág. 54

1.8 Nuevas formas de criminalidad

Una de las nuevas formas de criminalidad es la Ciberdelincuencia definida como las acciones que han sido cometidas mediante la utilización de un bien o servicio informático sin dejar a un lado que un servicio informático también es un bien jurídico que recibe protección por parte del ordenamiento jurídico, el desarrollo de la tecnología ha abierto una nueva posibilidad de delitos mediante la red, asesinatos y plagio de identidades así como también el abuso de redes.

Augusto Ciberech define a la Ciberdelincuencia como la serie de actividades delictivas realizadas con la ayuda de redes de comunicación y sistemas de información electrónicos o contra tales redes y sistemas.[9]

El tema que estoy desarrollando se interrelaciona con la criminología debido a que dentro de nuestro círculo social la Ciberdelincuencia se ha convertido en un problema social ya que los sujetos activos se aprovechan de la tecnología en este caso de la web para cometer acciones delictivas, a veces se hacen pasar por amigos o sutilmente llegan a las personas para obtener información de ellas, en el mundo entero se han dado muchos casos impactantes de como los ciberdelincuentes que son personas con problemas mentales acosan primeramente a la víctima y luego se obsesionan, crean en su mente cosas con ella y las matan sin contemplación alguna porque saben que no existe relación alguna entre ellos, en la actualidad hemos escuchado

[9] CIBERECH Augusto, *"La Ciberdelincuencia y sus consecuencias",* Editorial Sónico, México D.F., Pág. 156

por la televisión y radio muchos casos impactantes de cómo estas personas actúan mediante el internet a través de las redes sociales como Facebook, Twitter, MySpace, Sonico, msn; actualmente la mayoría de los adultos, jóvenes y niños crean cuentas en estas páginas y suben todo tipo de fotos y aún ponen todos sus datos personales sin escapárseles ninguno y aceptan como amigos a todo tipo de personas aún sin conocerlos.

Para algunas personas los ciberdelincuentes parecerán unos tontos pero en realidad son muy hábiles e inteligentes porque armar planes tan minuciosos no lo hace cualquiera, esto quiere decir que son muy inteligentes pero fuera de control, algunos psicólogos diagnostican que se debe a una niñez y adolescencia traumáticas. Lo que constituye una medida de disuasión en el mundo real pero inexistente en el virtual.

Los ciberdelincuentes como sujetos activos tienen como principal objetivo el beneficio económico puesto que a través de sus acciones delictuosas buscan lucrar lo que se traduce en la afectación de la esfera jurídica del ser humano. Parece irónico mencionar que opera bajo los principios sobre los cuales se rigen los negocios, por ejemplo: la rentabilidad, facilidad de uso, gestión de riesgos y atención a mercados emergentes, funcionando las veinticuatro horas del día a cualquier precio.

La ciberdelincuencia es sumamente rentable para las personas que se dedican a este acto delictivo comienzan con la extorsión de sus víctimas, roban todo lo que pueden y finalmente asesinan a su víctima sin piedad alguna.

1.8.1 Factores que incrementan la cibercriminalidad

- Riesgo: Uno de los factores que son clave en el incremento de la ciberdelincuencia es que el riesgo es mínimo puesto que no es fácil detener a los sujetos activos de esta.
- Innumerables servicios. Los innumerables servicios disponibles a través de Internet permiten que la mayoría de las personas se adapten al uso de estos contribuyendo al éxito de la Ciberdelincuencia.
- Redes sociales. Los más conocidos y usuales (Facebook, MySpace, Bebo, etc.), Servicios Web (Google, Yahoo!, MSN, Menéame, etc.), blogs o foros cada día incrementan el número de sus usuarios a la interactividad que ofrece este tipo de Webs.
- Facilidad de acceso. Un ejemplo claro lo observamos en la facilidad de descarga de los drivers para accesar a redes sociales, blogs, foros, entre otros.
- Las personas no tomamos conciencia de que estas redes sociales nos pueden causar mucho daño a la larga, ya que es muy peligroso porque a través de estas los ciberdelincuentes hacen de las suyas.

1.9 Características de los delitos cibernéticos

Actualmente los ciberdelincuentes construyen botnets, para robar contraseñas y datos confidenciales, y hacerse pasar por amigos o por personas conocidas. Los delitos cibernéticos de acuerdo a George Sprigh Agustín se caracterizan principalmente por:[10]

[10] SÜTHERLAND, Edwin, *" Cibercriminalidad",* Editorial Nuevo México, México D.F. 2003,

1) Masividad: se refiere a la capacidad de afectar la esfera jurídica a miles de personas con un sólo clic, como lo es en la figura delictiva phishing, que se visualiza en una estafa.

2) Perdurabilidad: se refiere a que perdura en el tiempo y sigue circulando, ejemplo la pornografía infantil.

3) Mutabilidad. Dadas las características de la prueba tecnológica, nadie nos puede garantizar que una CPU que se incauta hoy sea la CPU que se analice posteriormente.

4) Los cibercriminalidad precisa información traducida de ceros y unos y convertirla en información inteligible.[11]

Los delitos cibernéticos en 1943 fueron concebidos como "delitos de Cuello Blanco" por el criminólogo norteamericano Edwin Sütherland. Los denominaba así porque se requería de un determinado conocimiento y posición ocupacional para poder llevar a cabo este actuar, y con ello un cierto status socio-económico; en cambio actualmente cualquier persona con medianos conocimientos de informática puede llegar a ser un delincuente informático. Actualmente se les denomina "Delitos de Cuello Dorado" por la gran vistosidad con que se maneja esta figura delictiva, y la gran relevancia que tiene su proceder en comparación con las restantes figuras delictivas que son manejadas por los ordenamientos penales, por sus dañinas consecuencias. (castro, 2000)

[11] VELASCO, Angelino, *"Ciberdelincuentes",* Editorial Mundial, 2da Edición, México D.F. 2008, Pág. 135.

CAPITULO II

SUJETOS DE LA DELINCUENCIA CIBERNETICA

2.1 Generalidades

Actualmente se realizan gran mayoría de quehaceres u operaciones a través de una computadora que por comparecencia personal. A Través de su centro laboral, su tarjeta de crédito, su correo electrónico, sus datos personales fichados en los registros y archivos nacionales, en la actividad tributaria, entre otros. Las ventajas que ofrece el empleo de esta nueva tecnología en la optimización de los servicios que se brindan en estas esferas mencionadas y en muchas más son incuestionables, objetivamente sabemos que tiene aspectos negativos por lo que estamos a expensas de ser víctimas de las acciones antijurídicas que se lleven contra estos medios informáticos, los ciberdelincuentes o sujetos activos del delito pretenden saciar sus necesidades.

2.2 Sujetos activos

Sujeto activo: como la persona que a través de una acción u omisión transgrede y lesiona a otra en su esfera jurídica. Las personas que cometen los "Delitos cibernéticos" son aquellas que poseen ciertas características que no presentan el denominador común de delincuente, debido a que los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso de los sistemas informatizados, aun cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos. Con

el tiempo se ha podido comprobar que los autores de los delitos informáticos son muy diversos y que lo que los diferencia entre sí es la naturaleza de los delitos cometidos.[12] De esta forma, la persona que "entra" en un sistema informático sin intenciones delictivas es muy diferente del empleado de una institución financiera que desvía fondos de las cuentas de sus clientes. Los sujetos activos pueden ser:

A) Persona dentro de una organización:

Autorizados para ingresar al sistema (ejemplo: miembros legítimos de la empresa que acceden a cuentas corrientes o al departamento de personal).

No están autorizados a ingresar al sistema (ejemplo: personal contratista, aseo, eventual, etc.)

B) Personas fuera de la organización:

Autorizadas para ingresar al sistema (ejemplo: soporte técnico, soporte remoto de organizaciones de mantenimiento de software y equipos, etc.)

No están autorizados para ingresar al sistema (ejemplo: usuarios de Internet o de acceso remoto, sin relación con la institución).

Un buen sistema para fiscalizar la seguridad informática debe considerar todas las categorías anteriormente señaladas. Estos riesgos se controlan con los denominados firewalls o paredes de fuegos.

Al instalar unos buenos cortafuegos o firewall se puede eliminar las amenazas a la seguridad del sistema. Estos actúan como un escudo o barrera entre la red interna y el exterior y proveen un nivel de seguridad

[12] CAMPOLI, Gabriel, Andrés, "*Hacia una correcta hermenéutica penal delitos informáticos vs. delitos electrónicos"* AR: Revista de Derecho Informático núm. 048, julio de 2002

más allá de la protección por contraseñas o passwords. Los sujetos involucrados en la comisión de un delito cibernético reciben la denominación de sujetos activos.

2.2.1 Características de los sujetos activos

Como consecuencia de los parámetros a seguir por las personas que llevan a cabo este delito, asociamos que poseen características como:

- Listos
- Decididos
- Motivados
- Aceptan un retorno tecnológico

El termino Hackers es una denominación de los sujetos activos, con el que se define a las personas dedicadas, por afición u otro interés, a violar programas y sistemas supuestamente impenetrables, y apenas constituyen una muestra de la nueva faceta de la criminalidad.[13]

2.3 Clases de delincuentes cibernéticos

De acuerdo al comportamiento de los sujetos activos los podemos clasificar de la siguiente forma:

- El delincuente silencioso o tecnológico. Producto de la falta de información se les nombra así a todos sin tener en cuenta la diferencia implícita que lleva su actuar y las consecuencias del mismo.

[13] DÍAZ, ARANDA, Enrique, *"Teoría de la informática",* Editorial Straf, México , 2006, Pág. 98

- Sombrero Negro: calificados como terroristas y mercenarios, usan sus conocimientos para acceder a bases de datos que y posteriormente las venden.
- Sombrero Gris: este tipo de piratas se dedicaba a demostrar cuanto sabía y cuál era su capacidad para vulnerar sistemas.
- Sombrero Blanco: detectan errores y fallas en los sistemas de seguridad y advierten como remediar el problema.

2.4 Tipos de delincuentes cibernéticos.

2.4.1 Piratas informáticos

Este apelativo es atribuido a las personas que hacen uso del software creado por terceros, a través de copias obtenidas ilegalmente, vale decir, sin permiso o licencia del autor. Al software no original se le denomina "copia pirata", pero en términos reales deber llamarse un software robado.

La palabra pirata, asociada al uso ilegal del software, fue nombrada por primera vez por William Gatees en 1976, en su "Carta abierta a los Hobistas" mediante la cual expresó su protesta debido a que muchos usuarios de computadoras estaban haciendo uso de un software desarrollado por él, sin su autorización. En todo el mundo el uso del software ilegal está sujeto a sanciones y penalidades, que se agravan cuando el pirata se convierte en un comercializador de software copiado ilegalmente para lucrar en beneficio propio.[14]

[14] GATEES, William*, "Los delincuentes cibernéticos",* Editorial Pizzara, México D.F. 2001, Pág.198

2.4.2 Phreaker:

El phreaker es una persona con amplios conocimientos de telefonía puede llegar a realizar actividades no autorizadas con los teléfonos, por lo general celulares. Construyen equipos electrónicos artesanales que pueden interceptar y hasta ejecutar llamadas de aparatos telefónicos celulares sin que el titular se percate de ello. En Internet se distribuyen planos con las instrucciones y nomenclaturas de los componentes para construir diversos modelos de estos aparatos.

2.4.3 Delincuente informático

Es la persona o grupo de personas que en forma asociada realizan actividades ilegales haciendo uso de las computadoras y en agravio de terceros, en forma local o a través de Internet. Una de las prácticas más conocidas es la de interceptar compras "en línea" a través de Internet, para que haciendo uso del nombre, número de tarjeta de crédito y fecha de expiración, realizan compras de cualquier bien, mayormente software, o hasta hardware y para lo cual proporcionan una dirección de envío, diferente a la del titular del número de la tarjeta de crédito que usan en forma ilegal.[15] También es un delincuente informático el "pirata" que distribuye software sin contar con las licencias de uso proporcionadas por su autor o representantes, pues no solo atenta contra la propiedad intelectual, provocando la fuga de talentos informáticos, se enriquece ilícitamente y es un evasor de impuestos.

[15] J. HUERTA, Marcelo, *"Delitos informáticos",* Editorial Porrúa SA., Quinta edición, México D.F., 2000, Pág. 115

2.5 Sujetos adictos a la Tecnología

Lo que caracteriza a una persona con adicción es que este es el centro de su vida y ha perdido el control ante ella. Si no puede realizar una conducta determinada. Solo les interesa aquello que se relaciona con su adicción, el resto de las cosas no le interesan. Pareciera que el resto del mundo no le interesa, a excepción de la conducta adictiva y delictiva en la que está implicado. Aquello que es bueno y útil se puede convertir en malo y excesivo sino hay un adecuado control de lo que hace. Algunas personas tienen momento de descontrol de su vida. Es indudable lo que han representado en cuanto a progreso para la humanidad la mayoría de los desarrollos tecnológicos. Pero esto no ocurre con todas las personas, aquello que es bueno y útil se puede convertir en malo y excesivo si no hay un adecuado control sobre el uso que se hace. En el caso particular que nos ocupa las personas se convierten en adictas del internet al usar anómalamente una conexión a internet, la fascinación inicial por el internet puede llevar a tiempos de conexión altos al principio, por la novedad, pero luego tiene que regularse a un tiempo prudente y normal. Se considera que una persona que esté conectada más de cinco horas al día, por el mero hecho de estar no porque lo necesita para su trabajo, estudios o alguna investigación tiene problemas con el internet. Además de que podría añadirse una utilización solitaria, sin contacto con personas a su alrededor, la utilización de chats durante numerosas horas, sin ver personas realmente, sin saber como es o como piensa de verdad provoca que esta persona sea un sujeto adicto y pasivo de un delito cibernético. Por tanto una de las reglas de oro que se debe aplicar cuando se hace el uso del internet es solo contactar con personas conocidas. (Juventino, 2004).

Una de las posibilidades que provoca adicción es la conexión con otras personas a través del chat mediante el cual se intercambian puntos de vista, pero hay varios tipos de chats que se orientan al ocio y al tiempo libre, en los que destacan los que tienen como objetivo buscar relaciones con otras personas de todo tipo, sin considerar que la relación cara a cara nuca será la misma que la que se establece a través de una computadora.

Hoy sabemos que aquellas personas que utilizan en exceso el chat suelen tener problemas asociados con la depresión, ansiedad, descompensación emocional o alteraciones en el sueño, problemas de soledad, de falta de habilidades sociales o no saben comunicarse adecuadamente con los demás. Todo esto lo suplen con el chat al comunicarse con personas virtuales, pero que se debe evitar o por lo menos ser conscientes de que pueden ser víctimas de algún delito cibernético.

El café internet se ha convertido para algunas personas en su segunda casa. Los café internet han proliferado mucho en pocos años, ya que en ellos se encuentran computadoras potentes, pantallas deslumbrantes y precios asequibles, siempre que no se le dediquen horas y horas, ya que la mayoría de las personas tienen como problema el uso excesivo del internet.

2.6 Sujetos pasivos

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 cibernéticos" las víctimas pueden ser individuos, instituciones crediticias, gobiernos, etcétera que usan sistemas automatizados de información, generalmente conectados a otros.

El sujeto pasivo del delito que me ocupa, es sumamente importante para el estudio de los "delitos cibernéticos", ya que mediante él podemos conocer los diferentes ilícitos que cometen los delincuentes cibernéticos, con objeto de prever las acciones antes mencionadas debido a que muchos de los delitos son descubiertos casuísticamente por el desconocimiento del modus operandi de los sujetos activos.[16]

Dado lo anterior, "ha sido imposible conocer la verdadera magnitud de los "delitos cibernéticos", ya que la mayor parte de los delitos no son descubierto o no son denunciados a las autoridades responsables" y si a esto se suma la falta de leyes que protejan a las víctimas de estos delitos; la falta de preparación por parte de las autoridades para comprender, investigar y dar tratamiento jurídico adecuado a esta problemática; el temor por parte de las empresas de denunciar este tipo de ilícitos por el desprestigio que esto pudiera ocasionar a su empresa y las consecuentes pérdidas económicas, entre otros más, trae como consecuencia que las estadísticas sobre este tipo de conductas se mantenga bajo la llamada "cifra oculta" o "cifra negra".

[16] BAULLE, Faustino*," Esquema de los delitos cibernéticos",* Ediciones Botos, México 1999, Pág. 73

2.7 Vulnerabilidad de los sujetos pasivos

Resulta importante analizar que los sistemas informáticos, pueden entregar datos e informaciones sobre miles de personas, naturales y jurídicas, en aspectos tan fundamentales para el normal desarrollo y funcionamiento de diversas actividades como bancarias, financieras, tributarias, previsionales y de identificación de las personas.

Además la existencia de bancos de datos, empresas o entidades dedicadas a proporcionar, si se desea, cualquier información, sea de carácter personal o sobre materias de las más diversas disciplinas a un Estado o particulares; el estado es el garante de resguardar los valores colectivos, bienes jurídicos y en general a la esfera jurídica de todos los seres humanos a través del ordenamiento jurídico institucional, que como lo he mencionado durante el desarrollo del presente tema no se cuentan con el ordenamiento jurídico fehaciente que proteja al individuo de ser vulnerado en su persona, bienes y patrimonio. Ya que la utilización indebida de los sistemas de información actualmente son con fines de espionaje. Al respecto, el autor en cita, señala (81, 1999): “Las acciones que afectan a los sujetos pasivos son la manipulación o el consentimiento indebido de individuos poco conscientes e irresponsables de los datos que dichos sistemas contienen”.

2.8 Bien Jurídico Protegido

El objeto jurídico es el bien lesionado o puesto en peligro por la conducta del sujeto activo. Jamás debe dejar de existir ya que constituye la razón de ser del delito y no suele estar expresamente señalado en los tipos penales. (Zanca, 1996)

2.8.1 Bienes Jurídicos protegidos en el Delito Cibernético

Dentro de los delitos informáticos, podemos decir que la tendencia es que la protección a los bienes jurídicos, se le haga desde la perspectiva de los delitos tradicionales, con una re-interpretación teleológica de los tipos penales ya existentes, para subsanar las lagunas originadas por los novedosos comportamientos delictivos. Esto sin duda da como regla general que los bienes jurídicos protegidos, serán los mismos que los delitos re-interpretados teleológicamente o que se les ha agregado algún elemento nuevo para facilitar su persecución y sanción por parte del órgano jurisdiccional competente.

Pablo Palazzi dice que la información es una bien intangible constitucionalmente protegida. La protección de la información como bien jurídico protegido debe tomar en cuenta el principio de la necesaria protección de los bienes jurídicos que señala que la penalización de conductas se desenvuelva en el marco del principio de "dañosidad" o "lesividad".[17]

[17] PALAZZI, Pablo, *"Delito cibernético",* Editorial, Torrental, México D.F., 2006, Pág. 254

Una conducta sólo puede conminarse con una pena cuando resulta del todo incompatible con los presupuestos de una vida en común pacífica, libre y materialmente asegurada. Su origen directo es la teoría del contrato social, y su máxima expresión se encuentra en la obra de BECCARIA “Los Delitos y las Penas” (1738-1794). Se define como un bien vital, “bona vitae”, estado social valioso, perteneciente a la En conclusión podemos decir que el bien jurídico protegido en general es la información, pero esta considerada en diferentes formas, ya sea como un valor económico, como uno valor intrínseco de la persona, por su fluidez y tráfico jurídico, y finalmente por los sistemas que la procesan o automatizan; los mismos que se equiparan a los bienes jurídicos protegidos tradicionales tales como:

- El patrimonio, en el caso de la amplia gama de fraudes informáticos y las manipulaciones de datos que da a lugar.
- La reserva, la intimidad y confidencialidad de los datos, en el caso de las agresiones informáticas a la esfera de la intimidad en forma general, especialmente en el caso de los bancos de datos.
- La seguridad o fiabilidad del tráfico jurídico y probatorio, en el caso de falsificaciones de datos o documentos probatorios vía medios informáticos.
- El derecho de propiedad, en este caso sobre la información o sobre los elementos físicos, materiales de un sistema informático, que es afectado por los de daños y el llamado terrorismo informático.

Por tanto el bien jurídico protegido, acoge a la confidencialidad, integridad, disponibilidad de la información y de los sistemas informáticos donde esta se almacena o transfiere.

CAPITULO III:

CONSIDERACION TECNICA Y METODO PARA EVITAR LOS DELITOS CIBERNETICOS

3.1 Consideraciones

Es importante tener en cuenta que mi visión a estas alturas de la investigación no ha sufrido ningún cambio, pues si bien, han estallado algunas complicaciones en la investigación, existe algo que me motiva seguir con la misma, es la necesidad que existe en la sociedad de legislar un procedimiento para preservar correctamente los delitos cibernéticos; es decir, la importancia que tiene el legislar un procedimiento a seguir para los delitos cibernéticos, en el bagaje de prerrogativas que forman el ámbito colectivo se busca que se termine con la impunidad debido al mal empleo de personal incapacitado. Por lo que la investigación no puede ser modificada, mucho menos cuando se han encontrado puntos por los que resulta viable y acertado el fin perseguido en este estudio.

Creo que es importante recordar que en el capitulo primero de este documento, aporto un concepto de lo que considero, debe de tenerse en cuenta para la comprensión del tema, que estoy por concluir y que transcribo en estas líneas: **delitos cibernéticos "**Aquellas acciones que han sido cometidas mediante la utilización de un bien o servicio informático, sin dejar a un lado que un sistema informático también es un bien jurídico que recibe protección por parte del ordenamiento jurídico".

Es momento de formular algunos argumentos que resultan de la investigación que he detallado en hojas precedentes, que sin duda son interesantes, en la búsqueda de conocimiento y fundamentos que permitan al lector y al investigador, formar una plataforma de adopción y apoyo a la propuesta de legislar un procedimiento a seguir para preservar correctamente los delitos cibernéticos.

3.2 Catalogo de los delitos cibernéticos.

Para comenzar a hablar de los delitos cibernéticos es necesario hacer alusión a al nombre de Ameba Maltesa que es un virus informático, un tipo de programa que puede infectar el software de tu ordenador y destruir datos. La creación de virus es un delito cibernético. Los virus son programas creados deliberadamente para destruir datos y que pueden esconderse en el sistema de un ordenador. Pueden corromper todos tus datos y hacerlos inutilizables. Una vez que el virus está en el ordenador y si forma parte de una red se extenderá. La mejor forma de acabar con los virus son los antivirus.

El virus Miguel Ángel se programó para que actuara coincidiendo con el aniversario del nacimiento del pintor italiano. Ataco sistemas informáticos de todo el mundo, inutilizando los datos de los discos duros. El virus del Golfo, los Estados Unidos utilizaron un virus informático contra Irak durante la guerra del Golfo. Espías de Estados Unidos pusieron un chip infectado en una impresora vendida a los iraquíes. El chip había sido diseñado para corromper el sistema de mainframe que controlaba el centro de control militar iraquí. El virus Cascada cuando este virus infecta un ordenador, hace que todas las letras de un documento caigan en cascada y queden apiladas en la parte de debajo de la pantalla. Como se

puede apreciar los virus afectan importantemente los ordenadores y hacen que la información se pierda.[18]

VIRUS INFORMATICOS Y MALWARE

[18] WWW.Google.com.mx.12 de diciembre del 2012, MORALES SARMIENTO, Autor, pág. 42

3.2.1 El delito informático

Se concibe como un crimen electrónico, que agobia con operaciones ilícitas realizadas por medio de Internet o que tienen como objetivo destruir y dañar ordenadores, medios electrónicos y redes de Internet. El delito informático a su vez incluye delitos tradicionales como el fraude, el robo, chantaje, falsificación y la malversación de caudales públicos en los cuales ordenadores y redes han sido utilizados, ataques a sistemas, robo de bancos, ataques realizados por hackers, violación de los derechos de autor, pornografía infantil, pedofilia en Internet, violación de información confidencial. La sucesión reiterada de estos delitos poco a poco se ha sofisticado.

A su vez los delitos cibernéticos se pueden clasificar en dos grupos: [19]

1.- Crímenes que tienen como objetivo redes de computadoras, por ejemplo, con la instalación de códigos, gusanos y archivos maliciosos (Spam), ataque masivos a servidores de Internet y generación de virus.

2.- Crímenes realizados por medio de ordenadores y de Internet, por ejemplo, espionaje, fraude y robo, pornografía infantil, pedofilia, entre los más comunes.

[19] CASSOU, RUIZ, Jorge Esteban, *"Cibercriminalidad",* UNAM, México 2003, Pág. 54

3.2.2. Crímenes específicos

El Spam o correos electrónicos, no solicitados para propósito comercial, es ilegal en diferentes grados. La regulación de la ley en cuanto al Spam en el mundo es relativamente nueva y por lo general impone normas que permiten la legalidad del Spam en diferentes niveles. El Spam legal debe cumplir estrictamente con ciertos requisitos como permitir que el usuario pueda escoger el no recibir dicho mensaje publicitario o ser retirado de listas de email.

3.2.3 Fraude

Consiste en inducir a otro a hacer o a restringirse en hacer alguna cosa de lo cual el criminal obtendrá un beneficio al alterar el ingreso de datos de manera ilegal. En este caso particular encontramos que el sujeto activo es el empleado de una empresa que conoce bien las redes de información de la misma y puede ingresar a ella para alterar datos, generar información falsa que los beneficie, crear instrucciones y procesos no autorizados o dañar los sistemas. Un ejemplo muy conocido es el ocurrido en la empresa de Master Card anunció esta semana que la falla en los sistemas de seguridad, ocurrió en la empresa CardSystems Solutions, de Atlanta, que procesa pagos a bancos y comerciantes. Al mismo tiempo indicó que cerca de 14 millones de tarjetas llevan su nombre y las otras el de distintos emisores, como Visa Internacional, American Express, por lo que hasta 22 millones de tarjetas Visa podrían verse afectadas.

Afortunadamente para los clientes de MasterCard, el pirata informático sólo accedió a los números de las mismas y no a otros datos como los

dígitos de la Seguridad Social (equivalente al número de RUT nuestro) o la fecha de nacimiento de los clientes, datos usados frecuentemente por los usuarios que no asignan la importancia a la seguridad. Según un informe publicado recientemente por la firma de Massachusetts Aite Group, EU es el país desarrollado con mayores tasas de robo de identidad. Según la compañía, el uso fraudulento de datos individuales es siete veces mayor en Estados Unidos que en Europa y Japón.

3.2.4 Pishing

Es una modalidad de fraude informático diseñada con la finalidad de robarle la identidad al sujeto pasivo. El delito consiste en obtener información tal como números de tarjetas de crédito, contraseñas, información de cuentas u otros datos personales por medio de engaños.

Este tipo de fraude se recibe habitualmente a través de mensajes de correo electrónico o de ventanas emergentes. El robo de identidad es uno de los delitos que más ha aumentado. La mayoría de las víctimas son golpeadas con secuestros de cuentas de tarjetas de crédito, pero para muchas otras la situación es aún peor. En los últimos cinco años 10 millones de personas han sido víctimas de delincuentes que han abierto cuentas de tarjetas de crédito o con empresas de servicio público, o que han solicitado hipotecas con el nombre de las víctimas, todo lo cual ha ocasionado una red fraudulenta que tardará años en poderse desenmarañar.

3.2.5 Hostigamiento

Se dirige de manera específica a un individuo o grupo con comentarios derogativos a causa de su sexo, raza, religión, nacionalidad, orientación sexual. Esto ocurre por lo general en canales de conversación, grupos o con el envío de correos electrónicos destinados en exclusiva a ofender.

3.2.6 Tráfico de drogas

Actualmente el internet facilita la comunicación sin necesidad de tener contacto personalmente, por este motivo las mafias han ganado su espacio de operación haciendo que los posibles clientes se sientan más seguros con este tipo de contacto aunado a que el Internet posee toda la información alternativa sobre cada droga, lo que hace que el cliente busque por sí mismo la información antes de cada compra. Las drogas son vendidas ilegalmente a través de emails codificados incluso concertan citas a través del internet.

3.2.7 Terrorismo virtual

El terrorismo virtual se ha convertido en un delito informático, cuya principal caracterización es atacar masivamente el sistema de ordenadores de una empresa, compañía, centro de estudios, oficinas oficiales. Un ejemplo claro fue el caso muy mencionado de Owen Thor Walker (AKILL), de Nueva Zelandia quien en compañía de otros hackers, dirigió un ataque en contra del sistema de ordenadores de la Universidad de Pennsylvania en 2008.

La difusión de noticias falsas en Internet (por ejemplo decir que va a explotar una bomba en el Metro), es considerado terrorismo informático y es procesable.

3.3 Eficacia en la técnica de investigación respecto de los delitos cibernéticos

La técnica de investigación como tal no se encuentra establecida en ningún ordenamiento jurídico debido a la naturaleza virtual de los delitos informáticos, lo que ocasiona una tipificación confusa. La falta de cultura informática es un factor crítico en el impacto de los delitos informáticos en la sociedad en general. Los auditores informáticos no cuentan con un procedimiento o técnica de cómo seguir o determinar con claridad las evidencias de constitución de un acto delictivo cibernético. Lo que resulta cierto es que la policía, peritos, auditores informáticos y demás actores deben asegurar que las medidas de protección sean las adecuadas para

salvaguardar todos aquellos indicios que esclarecerán el hecho delictuoso.[20]

3.4 Reglas para proteger a los afectados con los delitos cibernéticos.

Debe crearse un procedimiento de auditoría que revise el uso de la red, servidores y sistemas aplicativos de forma periódica y el desarrollo de una política de uso de los recursos. El desarrollo de una política de seguridad comprende la identificación de los activos de la organización, identificación y evaluación de amenazas potenciales, análisis del riesgo, implementación de medidas preventivas para hacer frente a los riesgos.

Identificación de los activos de la organización: Consiste en la creación de una lista de todas las cosas que precisen protección. Hardware: computadores y equipos de telecomunicación. Software: programas fuente, utilidades, programas de diagnóstico, sistemas operativos, programas de comunicaciones.

Se proponen las siguientes reglas de protección:

1. En primer lugar se realizar la identificación y evaluación de amenazas potenciales
2. Análisis de Riego para cuantificar las amenazas potenciales para que sean establecidas las bases para una apropiada selección de costo eficiencia de los controles de seguridad.

[20] LANDAVERDE, M. L., SOTO, J. G. y TORRES, J. M. *"El internet como delito"* En revista mexicana de justicia, núm. 69, año 12, Junio 2000, Buenos Aires Argentina, Págs. 258 y 260

3. Implementación medidas preventivas para hacer frente a los riesgos, es decir, incluir documentos normativos, reglas, políticas, procedimientos de trabajo que consideren medidas preventivas y correctivas encaminadas a la práctica del delito informático, hacer uso de las tecnologías disponibles.

3.5 Los delitos cibernéticos y la policía

Al respecto la policía no tiene conocimiento estricto y adecuado de la postura que debe tomar ante el conocimiento de un hecho delictivo de carácter cibernético, la mayoría de las personas que fungen como policía no cuentan con la preparación adecuada aunado a que tienen nulo conocimiento sobre la tecnología y específicamente en el uso de la computadora a través del internet. (Antonio Saldaña Peña, 2002) Considero que en su contrato de trabajo se establezcan clausulas especiales sobre preparación y capacitación cuando se requiera para evitar actitudes negligentes. O segregación del personal, el establecimiento de un código ético de carácter interno en la organización 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.[21] En algunos países suelen tener policía especializada en la investigación de estos complejos delitos que al ser cometidos a través de internet, en un gran porcentaje de casos excede las fronteras de un único país complicando su esclarecimiento viéndose dificultado por la diferente legislación de cada país o simplemente la inexistencia de ésta.

[21] TÉLLEZ, J."Cibercriminalidad", Editorial Trillas, Segunda Edición, México D.F. 1999, Pág. 115 116 y 117

3.5.1 Ejemplos de delitos cibernéticos atendidos por FBI

Estafa de subasta de PlayStation en línea. Las víctimas de esta estafa reciben correos electrónicos no solicitados en donde se les informa que su anuncio de un Sony PlayStation y otros accesorios ha sido publicado. El mensaje incluso contiene un número de confirmación. Sin embargo algunas de las víctimas dicen no tener una cuenta para participar en subastas en línea.

El objetivo de esta estafa es adquirir información personal de las víctimas, incluyendo datos personales, contraseñas y números de tarjetas de crédito. Esta estafa ha existido desde el 2009.

Estafas de demandas colectivas masivas. Algunas víctimas han reportado recibir una carta de un despacho de abogados de California que les informa que son posibles demandantes en una demanda colectiva en contra de la compañía dueña de su préstamo hipotecario. El despacho de abogados promete varias cosas y ofrece servicios legales y de litigio a cambio de tarifas no reembolsables y pagadas por adelantado de entre $2,000 y $5,000.Sin embargo esto es una estafa. Los abogados que buscan a demandantes para juicios colectivos no solicitan comisiones por adelantado y típicamente se les paga una vez que ganan el juicio o llegan a un acuerdo a favor de sus clientes.

Correos electrónicos con información que parece ser oficial Varias agencias del gobierno así como oficiales de alto rango han sido el blanco de ataques de spam, o mensajes electrónicos no solicitados. Una nueva versión de estafas spam utiliza los nombres de oficiales del FBI así como unidades específicas dentro de la agencia. Los mensajes informan a las posibles víctimas que dos cajas con grandes cantidades de dinero fueron interceptadas en un aeropuerto internacional. Los fondos supuestamente pertenecen al gobierno de Nigeria. El mensaje

dice que las cajas contienen documentos que indican que la víctima es la dueña de los fondos. Se les pide a las víctimas contactar a los estafadores por correo electrónico y se les advierte de las consecuencias de no seguir las instrucciones. Se les pide no contactar a bancos o alguna otra institución. Los consumidores no deben responder a correos electrónicos que no fueron solicitados o hacer clic en los enlaces dentro del mensaje ya que podrían contener virus u otros programas malignos para la computadora.

Antecedentes caso X-TEAM

Todo comenzó el 25 de enero de 1998, cuando se cumplía un nuevo aniversario del trágico y lamentable crimen del reportero gráfico José Luis Cabezas. Ese mismo día, el site de la Corte Suprema de Justicia se veía la clásica (aunque también lamentablemente olvidada) foto de "No se olviden de Cabezas". Junto al emblema, se pedía el esclarecimiento del caso, firmado por un grupo de hackers autodenominado X-Team. Junto al emblema, se pedía el esclarecimiento del caso, firmado por un grupo de hackers autodenominado X-Team. La reacción de la Corte no se hizo esperar, y al día siguiente presentó una denuncia contra los NN que fue a parar al juzgado de Gustavo Literas, luego la causa la tomó Claudio Bonadio, y finalmente llegó a las manos de Sergio Torres. Así y todo, el X-Team no se detuvo, y el 25 de marzo de 1999 atacaron el site oficial de las Fuerza Aérea Argentina (hoy ya inexistente), denunciando el golpe de Estado de 1976.Tras un largo recorrido por distintos juzgados, el juez Torres finalmente determinó que en la Argentina no es delito sabotear (hackear) una página Web, basándose en que solamente "las personas, los animales, y las cosas están protegidos por el código penal".

Delitos Cibernéticos Internacionales

125 Ciber criminales arrestados en Estados Unidos Timothy Muris, director de la Comisión Federal de Comercio, se muestra orgulloso ante el éxito de la Operación llamada Ciber-sweep (ciber-barrida). “El ciberespacio no es lo mismo que el espacio exterior, y podemos seguir la pista y detener a cualquiera”. Desde que comenzara la operación el pasado uno de octubre, se ha descubierto que entre todas las estafas cometidas por estas personas, los ciber criminales se han embolsado más de 100 millones de dólares pertenecientes a unas 125.000 víctimas en los últimos meses, por lo que no es de extrañar que, además de la Comisión de Comercio, el FBI, el Servicio Secreto y hasta 34 abogados dirigidos por el Departamento de Justicia de Estados Unidos, fueran tras su pista.

Entre los casos abarcados, se encuentra el del diseñador John William Racine II, culpable de redireccionar el tráfico de la web de Al-Jazeera a la suya propia, donde se podía ver una bandera estadounidense. El fiscal ha pedido tres años de libertad vigilada y mil horas de servicio a la comunidad. Helen Carr ha sido declarada también culpable por simular correos de América On Line y enviarlos a sus clientes, pidiéndoles la actualización de sus datos de tarjeta de crédito.

Edward Fedora quiso vender una Medalla de Honor del Congreso a través de una subasta on line, a un precio inicial de 30.000 dólares. En los primeros nueve meses de 2003, el Centro de Quejas de Fraude de Internet, un proyecto común del FBI y National White Collar Crime Center, registró 58392 fraudes relacionados con Internet, que contrastan con las 48.000 denuncias registradas durante todo 2002. Dos adolescentes del poblado de Cloverdale, San Francisco (US)

fueron acusados de un sabotaje informático. Mediante una red de internet local (Netdex Internet Services), burlaron claves de seguridad e ingresaron a bancos de información esencial de varias agencias gubernamentales entre otras, una central de proceso de datos de la NASA donde habrían estado en contacto con el listado de guardias de seguridad, horarios de sus patrullas y varios secretos más. De esto se pueden sacar conclusiones sobre qué ocurriría si un grupo terrorista se apoderara de semejante información. Vladimir Levin. Fue condenado por haber ingresado a los centros de cómputos de algunos bancos efectuando transferencias de fondos en su beneficio por alrededor de 2.8 millones de dólares, aunque se afirma que un banco afectado manifestó haber perdido 10 millones de dólares. Alexei Lashmanov, considerado uno de sus ayudantes, fue condenado a cinco años de prisión y a pagar 250.000 dólares de multa por efectuar transferencias similares entre bancos estadounidenses, de Finlandia e Israel. El medio utilizado por estos últimos hackers para cumplir con su cometido no dista mucho de los ya citados, Levin trabajaba en una terminal informática de la empresa AO Sutnr, en St. Petersburg (Rusia), desde donde ingresó, entre otros, al Citibank Cash Management System. Una diferencia que la misma comunidad hacker se ocupa de remarcar es la siguiente: un hacker es simplemente alguien capaz de manejar con gran habilidad un aparato, no necesariamente una computadora, con el fin de sacarle más partido o divertirse. Los crackers, en cambio, utilizan mal sus conocimientos, y suelen meterse en problemas por eso.

No hay manera, hasta el momento, de impedir que los hackers o crackers intercepten las conexiones entre las oficinas gubernamentales y los centros privados de investigación.

3.6 Medios de prueba utilizados en la comprobación de los delitos cibernéticos

- 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.
- 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.[22]

3.7 Inmutabilidad de las pruebas para los delitos cibernéticos

El rastreo o trazabilidad: esto es, llegar desde el resultado a donde está el origen del ataque. Evitando la conculcación del sistema jurídico. Para ello se debe considerar que lo público se puede llevar como prueba ante los juzgados, pero para revisar los ficheros de un equipo informático privado se necesitas el permiso del titular o bien una orden judicial. Una de las

[22] REYNA, ALFARO, Luis, *"Medios de prueba cibernéticos",* Editorial Oxford, 2007, Pág. 378

técnicas más utilizadas para evitar la inmutabilidad de las pruebas es el clonado o volcado de los datos.

3.8 Promoción, control y evacuación de los medios de prueba.

El proceso probatorio es vital. Para estar frente al llamado Control de la evidencia digital. Es vital poder controlar la prueba para las partes afectadas. Es lógico analizar esto como la reconstrucción de los hechos. Cómo sucedieron, a quienes afectó y como poder demostrar ante los órganos jurisdiccionales quien son los sujetos activos responsables de estos ilícitos. Es importante que la prueba deba referirse, directa o indirectamente, al objeto de la investigación y ser útil para el descubrimiento de la verdad, además, se apreciará por los órganos jurisdiccionales observando las reglas de la lógica, los conocimientos científicos y las máximas de experiencia. Los parámetros indican que el juzgador debe estar muy atento sobre cualquier irregularidad que pueda cometerse. Es posible que no esté empapado de lo amplio del mundo de la Web, del comercio electrónico, la contratación informática, teniendo como obligación hacerse llegar de la información y conocimientos adecuados para emitir un juicio de si se trata de una simple facturación electrónica, superintendencia de entes de certificación, firma electrónica, que son muestra clara de evidencias relacionadas con ataques por virus. Ya que muchas de las personas que son jueces no tienen los estudios, ni las herramientas a la mano para poder trabajar con holgura y tranquilidad. Al respecto, el autor en cita, señala (380, 2007): “Siempre es clave estar apoyado por los ingenieros en informática, computación o sistemas que manejen el tema”. Por ello, es determinante que los peritos estén siempre muy actualizados.

3.9 Cadena de custodia

La cadena de custodia hace referencia a todos y cada uno de los pasos a seguir para salvaguardar las evidencias del hecho delictivo, sin conculcar o afectar a persona alguna. (Zanca, 1996) En las pruebas electrónicas no se tiene el problema que comúnmente se tiene en los otros delitos. En este caso los peritos de la materia trabajan sobre la copia, y la copia madre se custodia en el juzgado.

3.10 Impacto de los delitos cibernéticos

3.10.1 Impacto a nivel general

Los delitos cibernéticos representan una amenaza latente para la sociedad en general, generan la inseguridad institucional, provocando inestabilidad en las relaciones entre las personas, un ejemplo podría ser enviar un mensaje anónimo por correo electrónico dentro de una institución, hogar, entre otros, acusando falsamente a ciertas personas, generando con esto desconcierto, dudas sobre esas personal, creando inestabilidad emocional en el hogar, en la familia y en las instituciones. Desde fechas anteriores hasta la actualidad no se ha logrado reprimir conductas delictivas en el ámbito internacional ya que ni siquiera se cuanta con normas que reglamenten la conducta del sujeto agresor, si bien los acuerdos de cooperación internacional y los tratados de extradición bilaterales intentan remediar algunas de las dificultades ocasionadas por los delitos informáticos, sus posibilidades son limitadas. Los delitos cibernéticos constituyen una realidad de juegos lícitos e ilícitos, en donde es necesario el derecho para regular los múltiples efectos de una conducta de acción u omisión potencial en el medio social.

3.10.2 Impacto a Nivel Social

La práctica constante de delitos cibernéticos ha propiciado en la sociedad un escepticismo en la utilización de tecnologías de la información, las cuales pueden ser de mucho beneficio para la sociedad en general. Lo anterior veda el desarrollo de nuevas formas de hacer negocios. Las personas que no poseen los conocimientos informáticos básicos, son más vulnerables a ser víctimas de un delito, que aquellos que si los poseen. Más aun las personas de escasos recursos económicos al no tener conocimiento de las tecnologías son más vulnerables de conductas lesivas de su persona.

3.10.3 Impacto en la Esfera Judicial

Encontramos que no se tiene interés alguno en legislar un procedimiento adecuado para prevenir y evitar conductas lesivas de la esfera del ser humano en cuanto a la tecnología, técnicamente llamamos a ese tipo de conductas delitos cibernéticos, lo que se hace patente ya que aunque existen determinados pasos a seguir no se aplican en la realidad. Lo que ocasiona que el ejercicio de la acción penal en la Averiguación Previa no contenga todos los elementos de un tipo determinado para resolver un caso concreto, puesto que no se actúa de forma metodológica y científica para preservar eficazmente las evidencias que acrediten el delito cibernético. Más aun el desconocimiento del uso de la tecnología informática entorpece completamente la investigación, enjuiciamiento y condena de los transgresores.

CAPITULO IV: CONTROL ADECUADO DE LOS DELITOS CIBERNÉTICOS

4.1 Manejo de los delitos cibernéticos en la averiguación previa

La Averiguación Previa es una fase de investigación que le corresponde al Agente del Ministerio Público, para que éste, como órgano investigador la perfeccione, esto es, encontrar los elementos del cuerpo del delito de una conducta determinada sancionada por las leyes penales.

La averiguación previa puede tener detenido o no. En caso de que se cuente con detenido, se tiene un término de 48 horas, por tanto en esta etapa se debe valorar correctamente los indicios encontrados en el lugar de los hechos y de una forma pronta ya que se cuenta con término para no vulnerar en este caso la esfera jurídica del detenido. En el presente caso la determinación del Agente del Ministerio Público puede ser: l**ibertad bajo caución**, en la cual el detenido o detenidos deberán de garantizar su libertad; **libertad por vencimiento del plazo**, cuando llegado el término de las 48 horas al Ministerio Público le faltaron diligencias por practicar o bien no reunió los elementos suficientes para encuadrar el delito; y la **consignación con detenido**, esta quiere decir que el detenido será enviado al Reclusorio correspondiente. El término constitucional de 48 horas durante la Averiguación Previa se puede ampliar a 96 horas en los casos en que se cometan delitos por delincuencia organizada, y para que se perfeccione, deben participar tres o más personas. (Zanca, 1996).

La otra forma de poder iniciar una Averiguación Previa es sin detenido, donde únicamente el querellante o denunciante hace del conocimiento a dicha autoridad de una conducta probable de delito, donde ésta se llevará

a cabo en su investigación en una mesa de trámite; la determinación que el ministerio publico puede dar a conocer es el ejercicio de la acción penal y el no ejercicio de la acción penal, a través de ésta deja insubsistente la materia del delito.

Por lo anterior es que los es que la adecuada preservación de indicios de los delitos cibernéticos permitirán emitir una determinación técnica y eficaz dentro del proceso de la Averiguación Previa a efecto de sancionar adecuadamente a los sujetos activos del delito.

4.2 Hecho delictivo

Si queremos reconstruir, con cierta seguridad, un hecho delictuoso o identificar al infractor, es necesario, en primer lugar, preservar y conservar los indicios de la conducta delictiva. Esto es fundamental en la investigación criminalística, puesto que la falta de cumplimiento a cabalidad de esta etapa, puede facilitar la impunidad de un hecho[23].

Con la conservación adecuada de los indicios se lograra que el escenario del delito cibernético permanezca tal cual lo dejó el infractor, a fin de que toda la evidencia física conserve su situación, posición y estado original.

Pareciera absurdo que se haga uso de la criminalística para los delitos cibernéticos pero tienen una relación muy estrecha con la misma desde el

[23] RODRIGUEZ, MANZANERA, Lucia, *"Manual de las Ciencias Penales"*, Editorial, Porrúa, México D.F. 2000, Pág. 135

momento en que se deben preservar indicios de la acción u omisión motivo del delito cibernético. Por ello me permito tomar en consideración el Principio de Transferencia o Intercambio de Materias enunciado por Edmond Locard que señala que al cometerse un delito se realiza una visión rigurosa de elementos o materiales sensibles entre el autor, el lugar de los hechos y la víctima. (Campos, 2006)

4.3 Peritos

Perito (es toda persona a quien se atribuye capacidad técnico-científica, o práctica en una Ciencia o arte),[24] es un cuerpo elemental dentro de la investigación de Delito. La Procuraduría General de Justicia tiene una Dirección General de Servicios Periciales la cual cuenta con personal técnico-científico, especializado en diferentes áreas o disciplinas periciales. Los cuales presentan previo estudio, el análisis de las personas, objetos, mecanismos y hechos; un sustento científico que se interpreta en un Dictamen, traducido en una serie de puntos específicos, concretos y fundamentales, con bases científicas y técnicas que pueden ser sometidas a comprobación.

Resulta importante establecer una diferencia entre los términos más usados por los peritos.

Pericia. Es la capacidad, habilidad, talento, sagacidad, para desarrollar cualquier tarea ya sea técnico-científica o práctica,

Peritación. Es el procedimiento metodológico desarrollado y empleado por el perito para realizar la implementación de su tarea.

[24] MORENO, GONZÁLEZ, Rafael, *"Compendio de criminalística"*, Editorial, Porrúa, México 2002. Pág. 88.

Peritaje. Es el resultado metódico y estructural que nos conduce a la elaboración de un Dictamen o Informe que desarrolla el perito en el cual, previo examen de una persona, de una conducta o hecho.

Sabemos que todo personal que realiza una investigación, tiene la facultad y habilidad de desarrollarlo conforme a los elementos que se tengan, a la búsqueda de indicios que se recolectaron a las evidencias que se seleccionaron y sobre todo, conforme a los alcances de una investigación de altura que cumpla todos los requisitos de procedibilidad y guarde la sustentación técnica-científica del probable hecho delictuoso.

4.3.1 Perito Cibernético

Es un perito judicial que en su carácter de auxiliar de la justicia tiene como tarea primordial la de asesorar al juez respecto a temas relacionados con la informática. La función del perito cibernético consiste en el análisis de elementos cibernéticos, a efecto de salvaguardar un indicio útil para el litigio jurídico al que ha sido asignado. (Atico 2003)

Son una pieza importante dentro del presente tema, ya que si se logra una adecuada coordinación con el Agente del Ministerio Público se logrará una tipificación eficaz y correcta de la conducta lesiva cibernética. El perito también requiere de la necesidad de legislar un procedimiento adecuado para el control adecuado de los delitos cibernéticos El perito dictamina con la aplicación de tecnología y metodología científica respecto a cuestiones técnicas que son sometidas a su consideración por los órganos investigador y jurisdiccional[25].

[25] DE PINA VARA, RAFAEL, *"La Pericia"*, Segunda Edición, 2009, Editorial, Porrúa. Pág. 234.

El papel del Perito en cuanto a la necesidad de legislar un procedimiento para el adecuado control de los delitos cibernéticos es importante ya que gracias a ellos se tienen una pericia considerada por Betti como aquella actividad representativa destinada a comunicar al juez percepciones e inducciones obtenidas objetivamente merced a una apreciación técnica de la cosa, persona o actividad que constituye el objeto de la inspección directa en el proceso. [26] Lo que como he dicho anteriormente nos permite tener un conocimiento más especifico respecto de un delito cibernético lesivo de la esfera de los sujetos pasivos.

4.3.1.1 Deberes profesionales del perito

I. Ser consciente de las limitaciones de su capacidad científica.

Ser consciente de lo que se sabe y de lo que se ignora, es de suma importancia en materia pericial. Equivale a tener una brújula que indique, ante un problema de esta especialidad, el camino a tomar, a saber: en caso de contar con la experiencia y los conocimientos necesarios que permitan su solución, proceder inmediatamente a ello; en caso contrario, procurarse de inmediato toda la información y la experiencia necesarias, absteniéndose entre tanto de dictaminar. Para tomar atinadamente estas decisiones, el perito deberá contar con un poder desarrollado de autocrítica.

II. Ser metódico, claro y preciso en sus dictámenes

Al redactar su dictamen, el perito debe tener siempre presente que va dirigido a una persona no especializada en criminalística. En virtud, debe esmerarse en ser claro, preciso, conciso y sencillo.

[26] GONZÁLEZ, MORENO Rodrigo, *"Introducción a la criminalística*", Editorial, Porrúa, Pág. 25.

III. Mantener actualizados los conocimientos técnicos y científicos

El perito tiene la obligación de mantener al día su información en materia de su especialidad, debiendo consultar para ello las más recientes publicaciones.

IV. Colaborar eficazmente con las autoridades en el esclarecimiento de la verdad.

La misión del perito consiste en auxiliar a los encargados de procurar y administrar justicia en el descubrimiento de la verdad histórica de los hechos. Esto significa que cualquier desviación al respecto, deberá encontrar en el experto la más rotunda negativa.

V. Dictaminar sobre cuestiones técnicas y científicas sin emitir opiniones de carácter legal

El perito no debe invadir cercados ajenos, no debe salirse del campo que le es propio. Debe limitar su actuación al terreno que le corresponde.

VI. Actuar con imparcialidad, acuciosidad, dedicación y prudencia

El perito procurará desentrañar la verdad objetiva, el hecho objetivo, la cosa objetiva, sin deformarla ni tergiversarla para ceder a inclinaciones personales o a intereses inconfesables.

VII. Aplicar los métodos y las técnicas de la investigación científica en la búsqueda de la verdad.

Los problemas de orden criminalístico que el perito tiene que resolver, requieren de él determinada postura intelectual, caracterizada por una

actitud crítica, que sólo admite conclusiones cuando éstas se basan en la verificación. El propio perito procurará establecer firmemente el procedimiento general que debe seguir, el orden de las observaciones, experimentaciones y razonamientos. Una vez establecido el camino general por recorrer, señalará los procedimientos particulares o técnicas, en su mayoría de orden instrumental, que deberá aplicar para tal fin. En suma, el perito deberá proceder con todo rigor científico.

VIII. Fundar sus conclusiones sobre la verificación de los hechos

El perito siempre deberá verificar empíricamente sus enunciados, ya sea por medio de la observación o de la experimentación. Es importante hacer notar lo siguiente: la criminalística, como todas las disciplinas, necesita de la racionalidad, es decir, necesita que sus enunciados sean coherentes y no contradictorios.

IX. Escuchar y ponderar ecuánimemente, con espíritu abierto, las objeciones metodológicas y técnicas que cuestionen sus dictámenes

El perito deberá recibir de buena voluntad cualquier crítica que se haga a su dictamen, aceptando siempre lo que a la razón y a la verdad convenga. Con inteligencia y serenidad defenderá sus enunciados, respetando siempre las opiniones contrarias.

Al respecto, el autor en cita, señala (304, 2009): “Es fundamental excluir de la controversia estrecheces y prejuicios, así como evitar expresiones que puedan dar lugar a resentimientos”. Las discusiones deben circunscribirse estrictamente al plano de los hechos. En resumen, el perito no tendrá miedo a la crítica, porque la verdad es fuerte y acaba por imponerse.

4.3.2 Áreas de intervención de los peritos cibernéticos

1.- Sistemas automatizados de identificación. En esta los peritos localizan en una base de datos de una computadora una huella cuestionada para obtener, en su caso, antecedentes de un presunto delincuente. La provisión de material informático en algunas ocasiones es escasa pero por ningún motivo debe ser un obstáculo para el desarrollo de su trabajo.

2.- Traducción. Debidos a que los delitos cibernéticos tienen como ciberespacio territorial todo el mundo. Por lo que el perito tiene la responsabilidad de saber una infinidad de idiomas.

4.3.3 Con el dictamen pericial

El dictamen pericial es el examen y estudio que realiza el perito sobre el problema encomendado para luego entregar su informe o dictamen pericial con sujeción a lo dispuesto por la ley.[27] Este dictamen procede para conocer o apreciar algún hecho de influencia a través de conocimientos científicos, artísticos o prácticos.

Para que el dictamen pericial tenga validez, en primer lugar se tendrá que proponer al perito que intervendrá en determinado hecho, posteriormente se procederá a su nombramiento por el agente del Ministerio Publico, juez o tribunal, para posteriormente emitir su dictamen o informe pericial.

4.3.3.1 Estructura del dictamen pericial

1) La descripción de la persona, objeto o cosa materia de examen o estudio, así como, el estado y forma en que se encontraba.

[27] CANO, CAMACHO, Augusto, *"Estudios de criminalística",* Editorial, Esfinge, 3ra Edición, México D.F., 2003, Págs. 110-131

2) La relación detallada de todas las operaciones practicadas en la pericia y su resultado.

3) Los medios científicos o técnicos de que se han valido para emitir su dictamen.

4) Las conclusiones a las que llegan los peritos.

Se señalará día y hora para la entrega y ratificación del dictamen pericial (requisito esencial), puesto que si no es ratificado no tendrá validez; por tanto, no amparará técnicamente y no será útil durante la averiguación previa y el proceso en general. La prueba pericial tiene que ser apreciada y valorada con un criterio de conciencia, según las reglas de la sana crítica. Los Jueces y tribunales no están obligados a sujetarse al dictamen de los peritos. Es por esto que se dice "El juez es perito de peritos".

4.4 Implicaciones de los peritos y sus efectos

La actividad pericial queda a cargo y bajo la responsabilidad absoluta de los peritos quienes la desarrollarán de acuerdo a lo establecido en el artículo 175 del Código de Procedimientos Penales para el Distrito Federal, mismo que dice: “Los peritos practicarán todas las operaciones y experimentos que su ciencia o arte les sugiera y expresarán los hechos y circunstancias que sirvan de fundamento a su dictamen.”

Es decir, el Ministerio Público no dirigirá al perito en su función, se concretará a solicitar su auxilio, administrar a los peritos toda la información necesaria para que emitan su opinión, y a recibir y agregar a la averiguación los dictámenes o informes rendidos por el perito. El Ministerio Público se abstendrá por completo de dirigir o intervenir en la tarea del perito. Una vez que el perito emita y presente su dictamen o informe por escrito al Ministerio Público, éste hará constar tal hecho en la

averiguación previa, asentando la fecha y hora y agregará el dictamen o informe de peritos a la averiguación. (Atico 2003).

4.4.4 Función del Agente del Ministerio Público en los delitos cibernéticos

Es de vital importancia analizar las implicaciones que al respecto tienen los agentes del ministerio público, en cuanto a la necesidad de legislar un procedimiento para lograr un control adecuado de los delitos cibernéticos,

La mayoría de las veces cuando los peritos, los técnicos, y el agente del Ministerio Público están ante la presencia de un hecho delictuoso, no llevan a cabo un procedimiento de acuerdo a los lineamientos y pasos a seguir para preservar la evidencia física de dicho hecho. Puedo percatarme de que en la mayoría de los casos los agentes de policía, así como los elementos aledaños a la investigación y persecución de los hechos delictuosos, obstruyen el procedimiento a seguir para lograr el control adecuado de los delitos cibernéticos. Es decir el control adecuado de los delitos cibernéticos tienen **fin inmediato** el tratar de que en la medida posible se instituya un procedimiento que evite lesividades a los sujetos pasivos; y como **fin mediato,** allegarse de las evidencias e indicios que acrediten fehacientemente el delito cibernético Por lo que en este proyecto de tesis yo quiero darle solución al problema planteado, estableciendo los pasos a seguir, los métodos y técnicas idóneas, así como las medidas necesarias para el control y prevención de los delitos cibernéticos.[28]

[28] CASSOU, RUIZ, Jorge Esteban, *"Cibercriminalidad",* UNAM, México 2003, Págs. 209-289

4.5 Recomendaciones para no ser víctima de delitos cibernéticos

Cada día aparecen nuevas expresiones de la criminalidad y actualmente muchas de ellas están vinculadas al uso de las nuevas tecnologías traducidas como acciones delictuosas cibernéticas por lose deben implementar acciones preventivas que contribuyan con la seguridad de las familias, padres, alumnos, instituciones educativas, empresas y sociedad en general que utilizan los instrumentos fabricados para el uso y aprovechamiento de las herramientas relacionadas con la comunicación y la informática.

4.6 Recomendaciones para los padres

- La utilización de herramientas de eliminación de software malintencionado para buscar, prevenir, detectar y eliminar este tipo de programas maliciosos como por ejemplo un antivirus y una firewall.
- Evite utilizar el servicio de banca en línea en cafés Internet o centros de negocios en hoteles, toda vez que esos equipos no siempre cuentan con software de seguridad y son blanco fácil de personas que tratan de obtener datos confidenciales.
- Procure usar un seudónimo y evite colocar el nombre, fotos y dirección electrónica de sus hijos en guías y perfiles públicos, a fin de proteger su identidad.
- No abra correos electrónicos de remitentes desconocidos ni archivos ejecutables porque pueden contener virus que dañen a su computadora y a todos sus archivos.
- Establezca, junto con sus hijos, la hora y reglas del uso de Internet y procure que naveguen bajo su supervisión, porque no sabe qué

información puedan bajar y corren el riesgo de que abran páginas con pornografía.

4.7 Recomendaciones para los niños y adolescentes

- No confiar por completo en la veracidad de la información encontrada en internet.
- No0 conectarse al internet por muchas horas seguidas durante el día ya que podría generar comportamientos antisociales y de aislamiento
- Antes de asociarte a un sitio de redes sociales, analiza detenidamente las diferentes opciones que te ofrecen.
- Piensa bien antes de colocar tu foto en el sitio Web ya que podría ser alterada y difundida.
- Ser prudentes si un nuevo amigo que has conocido por la red desea conocerte personalmente, si lo haces anda acompañado de un adulto, que la reunión sea de DÍA y en un lugar público, aunque esto no es nada recomendable
- Cuando veas o recibas algo en Internet que te haga sentir incómodo/a o amenazado/a, debes hablar inmediatamente con tus padres, para que den aviso a las autoridades.
- Por ningún motivo respondas a mensajes o avisos de boletines electrónicos que sean desconocidos, sugestivos, obscenos, agresivos o amenazantes o que te hagan sentir incómodo, o mensajes atractivos que indiquen que eres ganador de un sorteo para evitar fraudes y proteger tu intimidad e integridad.

- Nunca debes publicar información personal como número telefónico familiar o celular, dirección o nombre de tu escuela.
- Comparte tus contraseñas solo con una persona de tu confianza.
- Observa siempre un buen comportamiento en línea y no hagas nada que pueda molestar o enojar a otras personas o que sea ilegal.
- Deja que tus padres sepan tu nombre de inicio de sesión en Internet y las direcciones de los chats que visitas.

4.8 Recomendaciones para los docentes

- Evite bajar software gratuito ya que la mayoría contienen spyware (programas espía) que se instalan automáticamente en su computadora.
- No utilizar programas que ayuden a filtrar el contenido de sitios de Internet.
- Revisar su máquina periódicamente y recurrir a técnicos especializados para que la limpien de todo tipo software malicioso.
- Averiguar sobre las opciones de privacidad de la información que le brinda su proveedor de servicios de Internet.
- Mantener una supervisión del uso de Internet al interior de la escuela.
- Vigilar a sus alumnos cuando naveguen en Internet para que no proporcionen sus datos personales o los de su familia.
- Prohíba el uso de celular al interior de la escuela, ya que puede usarse para comunicarse inadecuadamente con personas adultas que pueden maltratar al menor.

Las recomendaciones vertidas nos ayudan a tener conciencia de cómo utilizar adecuadamente el internet para evitar una amenaza futura proporcional a los adelantos de las tecnologías informáticas.

4.9 Aplicación de un simulador con tarjeta de adquisición de datos.

Aplicación de un simulador con tarjeta de adquisición de datos para verificar el comportamiento de comunicación serial RS-232 con la PC, midiendo los fenómenos físicos denominados voltaje y corriente, para la aplicación a los dispositivos de manejo. La tarjeta de adquisición de datos, basada en la comunicación por PC, utiliza una combinación de diferentes aplicadores del simulador estableciendo el software de aplicación con la PC para realizaron funciones de comunicación segura, es decir con medidas de protección para los usuarios. La tarjeta de adquisición de datos maneja señales, sensores, actuadores, acondicionamiento de señales, motores en CD, servomotores. Se construyó esta interfaz de comunicación de adquisición de datos para la protección de los cibernéticos con un puerto paralelo de 8 bits de entrada y 8 bits de salida con comunicación serial hacia la PC, ofrece un sin número adicional de aplicaciones por desarrollar para el usuario, trabaja con la programación Labview que emite simulaciones graficas con detectores de los sujetos activos actores de acciones ilícitas que vulneren a los cibernéticos con fines lícitos. La etapa de salida es el conjunto de elementos que permiten conectar la tarjeta de adquisición de datos con la PC, a través de buffers digitales incluidos en el circuito convertidor, hasta un interfaz RS-232, Rs-485 o Ethernet para conectar a un ordenador o estación de trabajo, en el caso de sistemas de adquisición de datos comerciales. Debido a que es una necesidad primordial en cuanto a la protección y seguridad de los cibernéticos. El Micro controlador es uno de los

dispositivos electrónicos programables más sofisticados, lo que es fundamental para los grandes adelantos tecnológicos en casi todos los campos de la industria. (Sila, 2000)

Es necesario estar preparado en el desarrollo de aplicaciones de simulación como en la programación de software para el desarrollo de dispositivos de hardware, para lograr innovaciones en la capacidad de creación de dispositivos de protección ya que a su vez resulta necesario para el aprendizaje y manejo de los recursos computacionales con seguridad y certeza moral y jurídica.

La aplicación de simuladores trabaja con señales analógicas y digitales, es decir comienza con una señal digital a partir de una analogía, realizando las funciones de cuantificación y codificación.[29]

La cuantificación implica la división del rango continuo de entrada en una serie de pasos, de modo que para infinitos valores requiere de una codificación a partir de un código binario, de modo que las etapas del convertidor sean las necesarias para proteger la información que se procesa.

[29] ARABIA, LOZADA, Gaudencia, *"La informática",* Editorial, Latino Americana, 2010, México D.F., Pas. 68-230

Del código fuente del Micro controlador PIC, se envía la lectura proveniente de una codificación para la comunicación por medio del puerto serial, que es imprescindible para la configuración del simulador.

Con la utilización de simuladores de este tipo se lograra el manejo adecuado y seguro de aplicaciones como señales, sensores, actuadores, motores de CD, servomotores, a efecto de lograr una comunicación libre de vicios.

CONCLUSIONES

PRIMERA. La ocurrencia de delitos informáticos en las organizaciones alrededor del mundo no debe en ningún momento impedir que éstas se beneficien de todo lo que proveen las tecnologías de información sino por el contrario dicha situación debe plantear un reto a los profesionales de la informática, de manera que se realicen esfuerzos encaminados a robustecer los aspectos de seguridad, controles, integridad de la información.

SEGUNDA. En relación a los policías cibernéticos, es necesario capacitarlos para que éstos se alleguen de los conocimientos necesarios y logren un adecuado control de los delitos cibernéticos con las medidas y técnicas que se requieran.

TERCERA. Debe legislarse un procedimiento para lograr un control adecuado del delito cibernético de manera técnica y científica, para que dentro de la investigación previa se logre el esclarecimiento de los hechos y en su caso para ejercer o no, la acción penal.

CUARTA. La legislación sobre protección de los sistemas informáticos ha de perseguir acercarse lo más posible a los distintos medios de protección ya existentes, creando una nueva regulación sólo en aquellos aspectos en los que, basándose en las peculiaridades del objeto de protección, sea imprescindible.

QUINTA. Las consideraciones contenidas en la presente tesis, tienden a resolver un problema latente sobre los delitos cibernéticos. Primero, porque no se tiene normatividad clara y técnica que contribuya a realizar una prevención adecuada de los delitos cibernéticos y custodia de los indicios y en segundo lugar, porque con ello se facilitara el planteamiento de hipótesis y líneas de investigación, que, incluso se están previendo en la reciente reforma constitucional.

PROPUESTA

Al término de la presente investigación propongo que se regularicen en la normatividad del estado de Tlaxcala los delitos cibernéticos, es decir que se especifique cada uno de los elementos típicos para cada uno de las conductas cibernéticas y así de esta forma lograr una protección adecuada de los sujetos pasivos y la preservación adecuada de los indicios que el sujeto activo deje de su actuar.

Se busca la protección de los bienes jurídicos afectados por los delitos cibernéticos. Ya que con el auge de la tecnología las conductas delictivas incrementan en diversas modalidades.

P O S F A C I O

No pasa desapercibido en esta investigación que los delitos cibernéticos se han incrementado en manera desmedida, que las personas vulneradas con estos han sido afectadas considerablemente. Un procedimiento adecuado para evitar la consumación de los mismos constituyen eslabones contundentes en la integración de la averiguación previa, empero, como pruebas primigenias deben permanecer inalterables para su valoración futura como actualmente, se está diseñando para enjuiciamiento penal futuro.

Con base en lo anterior, considero que las recomendaciones vertidas en la presente tesis deben permanecer en la investigación de hechos cibernéticos y reflexionarse para su debida reglamentación como prueba anticipada.

Finalmente el saber científico es fuente inagotable del conocimiento, y considero que, las reflexiones que realicé en mi tesis servirán como referentes para estudios posteriores.

Agradezco la atención a la presente investigación.

FUENTES DE INFORMACIÓN.

Fuentes bibliográficas.

DURKHEIM, Emili, “Escritos Selectos, Introducción y selectos de Anthony Gidenns”, Editorial Buenos Aires, Nueva Visión, México D.F. 1993, Pág. 115

GRANDE, Edwin, “La cibercriminalidad en el presente”, Editorial Esquino, México D.F. 2003, Pág. 15

GUERRERO, MATÉUS, Fernanda, “Ciberdelincuencia”, Procuraduría General de la Nación. 2004, Pág. 218

CASSOU, RUIZ, Jorge Esteban, “Delitos informáticos en México”, Editorial Nueva imagen, 2009, Págs. 11- 19

GRANDE, Edwin, “La cibercriminalidad en el presente”, Editorial Esquino, México D.F. 2003, Págs.9-14

LÓPEZ, BETANCOURT, Eduardo, “informática”, México, Porrúa, 2004, p. 270.

TÉLLEZ VALDÉS, Julio, “Derecho informático”, 3ª. ed., México, McGraw-Hill, 2004, p. 163.

TERREL, Bynum, “Delitos informáticos”, Editorial Parris, 2 Edición, México D.F.2001, Pág. 54

CIBERECH Augusto, “La Ciberdelincuencia y sus consecuencias”, Editorial Sónico, México D.F., Pág. 156

SÜTHERLAND, Edwin, “Cibercriminalidad”, Editorial Nuevo México, México D.F. 2003,

VELASCO, Angelino, “Ciberdelincuentes”, Editorial Mundial, 2da Edición, México D.F. 2008, Pág. 135.

SÜTHERLAND, Edwin, “Cibercriminalidad”, Editorial Nuevo México, México D.F. 2003,

DÍAZ, ARANDA, Enrique, “Teoría de la informática”, Editorial Straf, México, 2006, Pág. 98

GATEES, William, “Los delincuentes cibernéticos”, Editorial Pizzara, México D.F. 2001, Pág.198

GUERRA, Marcelo, “Delincuentes Informáticos”, Editorial Oxford, México D.F., Pág. 132

J. HUERTA, Marcelo, “Delitos informáticos”, Editorial Porrúa SA., Quinta edición, México D.F., 2000, Pág. 115

MONTIEL, SOSA, Juventino, “Adicción a nuevas tecnologías”, Editorial, Espejo de Urania, México D.F., 2012, Pág. 21

BAULLE, Faustino,” Esquema de los delitos cibernéticos”, Ediciones Botos, México 1999, Pág. 73

PALAZZI, Pablo, “Delito cibernético”, Editorial, Torrental, México D.F., 2006, Pág. 254

MORENO, GONZALEZ, Rafael, “Delito informático”, Editorial, Nuevo México, 2003, Págs. 78-79

CASSOU, RUIZ, Jorge Esteban, “Cibercriminalidad”, UNAM, México 2003, Pág. 54

TÉLLEZ, J.”Cibercriminalidad”, Editorial Trillas, Segunda Edición, México D.F. 1999, Pág. 115 116 y 117

REYNA, ALFARO, Luis, “Medios de prueba cibernéticos”, Editorial Oxford, 2007, Pág. 378

Enciclomedia Microsoft Encarta 2002. 1993-2001 Microsoft, 24 febrero 2013, 14:45 hrs.

MORENO, GONZALEZ, Rafael, “La criminalística” 3ra Edición, Editorial Porrúa, México 2002, Págs. 74-112

RODRIHGUEZ, MANZANERA, Lucia, “Manual de las Ciencias Penales”, Editorial, Porrúa, México D.F. 2000, Pág. 135

MORENO, GONZÁLEZ, Rafael, “Compendio de criminalística”, Editorial, Porrúa, México 2002. Pág. 88.

DE PINA VARA, RAFAEL, “La Pericia”, Segunda Edición, 2009, Editorial, Porrúa. Pág. 234.

GONZÁLEZ, MORENO Rodrigo, “Introducción a la criminalística”, Editorial, Porrúa, Pág. 25.

CANO, CAMACHO, Augusto, “Estudios de criminalística”, Editorial, Esfinge, 3ra Edición, México D.F., 2003, Págs. 110-131

CASSOU, RUIZ, Jorge Esteban, “Cibercriminalidad”, UNAM, México 2003, Págs. 209-289

ARABIA, LOZADA, Gaudencia, “La informática”, Editorial, Latino Americana, 2010, México D.F., Pas. 68-230

(Juventino, 2004)http://ciberhabitat.gob.mx/noticias/mar2013

WWW.Google.com.mx.12 de diciembre del 2012, MORALES SARMIENTO, Autor, pág. 42

Fuentes hemerográficas

CAMPOLI, Gabriel, Andrés, “Hacia una correcta hermenéutica penal delitos informáticos vs. Delitos electrónicos” AR: Revista de Derecho Informático núm. 048, julio de 2002

LANDAVERDE, M. L., SOTO, J. G. y TORRES, J. M. “El internet como delito” En revista mexicana de justicia, núm. 69, año 12, Junio 2000, Buenos Aires Argentina, Págs. 258 y 260