UNIVERSIDAD DEL TEPEYAC

ESCUELA DE DERECHO

ANAISIS JURIDICO PARA PREVENIR Y COMBATIR LA DELINCUENCIA INFORMATICA

TESIS

QUE PARA OBTENER EL TITULO DE LICENCIADO EN DERECHO

PRESENTA

EDGAR ESPINOSA GONZALEZ

MEXICO, D.F. **2007**

Universidad Nacional Autónoma de México
UNAM
Biblioteca Central
Dirección General de Bibliotecas de la UNAM

UNAM – Dirección General de Bibliotecas
Tesis Digitales
Restricciones de uso

DERECHOS RESERVADOS ©
PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.

AGRADECIMIENTOS

Autorizo a la Dirección General de Bibliotecas de la UNAM a difundir en formato electrónico e impreso el contenido de mi trabajo recepcional.
NOMBRE: Edgar Espinosa González
FECHA: 28/09/07
FIRMA:

Aquello a lo que tienes miedo, es una clara indicación de lo siguiente que tienes que hacer.

Anónimo.

Agradezco:

A DIOS
Por todas las bendiciones recibidas.

A MIS PADRES
Por su apoyo incondicional a los cuales admiro respeto y amo.

A LA UNIVERSIDAD
Por la formación que recibí.

A MIS MAESTROS Y ASESOR
Por su tiempo y consejos.

A MI SEGUNDA FAMILIA
Que siempre me anima a seguir y a la que quiero mucho.

A MIS AMIGOS
Con los que he encontrado apoyo en los momentos difíciles

Y a todas las personas que directa o indirectamente me impulsaron a concluir con este esfuerzo mi eterna gratitud por haberlo hecho posible y no quedara en el olvido.

RESUMEN

El auge de la tecnología, la utilización de sistemas y redes de información, es lo que se ha adoptado por todo el mundo generando así, la interconexión entre todos los países, dichas redes dan soporte a muchas áreas estratégicas dentro de un país, como son el de energía, comercio, bancarias y financieras, así como la prestación de servicios dentro de un Estado. Dichas actividades sirven como medio de intercambio de información y comunicación, al mismo tiempo estos sistemas y redes de información van quedando expuestos a un creciente numero de amenazas; por eso la importancia de analizar los aspectos que inciden en la delincuencia informática, ampliando así la visión del derecho informático a fin de perfeccionar el marco jurídico existente para la creación de leyes más efectivas que sirvan para disuadir y sancionar los ataques a las redes, dando como consecuencia redes más sólidas y seguras. No obstante aunque ya existe legislación, es necesario abundar más sobre el tema, ya que la tecnología avanza y no existe un marco sólido que lo regule corriendo el riesgo de ser blanco fácil de la delincuencia informática. Este tema se encamina al análisis de la legislación existente, y dar pie a que se realice una regulación integral de delitos informáticos; la cual incumbe a todos los países, ya que las redes informáticas no tienen fronteras, por tal razón es de gran importancia crear normas claras, que ayuden a los diferentes Estados a no limitar el alcance de la ley, creando tratados que persigan este delito, ya que bien sabemos que estos delincuentes siempre buscan sistemas en otros países, como intermediarios para después afectar su objetivo principal, lo cual permite esconder identidades y ubicación. Es un delito relativamente nuevo, ya que años atrás, no se tenía la facilidad de acceder a la tecnología que hoy se tiene la cual desgraciadamente han abierto las puertas a las actividades delictivas. La computadora se ha convertido en un elemento básico de la vida de una sociedad, por tanto, un blanco fácil para cometer ilícitos por delincuentes sin rostro que acceden a las mismas a través de redes informáticas y se apoderan de datos sin autorización, a esta actividad se le considera como un delito y rompe con los esquemas de una sociedad, la cual debe de ser castigada, mediante normas que protejan y prohíba el acceso a sistemas informáticos que eviten el apoderamiento de

información de manera ilícita. Analizando los aspectos generales de la delincuencia informática encontraremos un marco jurídico que prevenga y combata al delito informático, los cuales deben ser regulados mediante leyes que sirvan y sancionen las conductas que afectan a todas las áreas de un estado, contribuyendo con un marco legal para una mejor identificación de las conductas antisociales relacionadas con los medios informáticos logrando un marco legal que de seguridad y prevenga conductas antisociales.

ÍNDICE

INTRODUCCIÓN

En la actualidad, el auge de la utilización de los sistemas y redes de información, ha generado un aumento en las interconexiones entre los países, las redes de computadoras dan soporte a infraestructuras de importancia crítica en el campo de la energía, el transporte, áreas bancarias y financieras, desempeñan también un papel importante en las actividades de las empresas y en los mecanismos de prestación de servicios que el estado proporciona a los ciudadanos y a la comunidad empresarial, además de servir como medio de intercambio, información y comunicación.

Las tecnologías de diversos tipos, se van multiplicando y seguirán creciendo, al igual que el volumen y la sensibilidad de la información que se transmite de un lugar a otro, al mismo tiempo los sistemas y redes de información van quedando expuestos a un creciente número de amenazas, ni el comercio electrónico ni los mercados podrían desarrollarse sin redes de información sólidas y seguras que cuenten con la confianza del público.

Un elemento que sirve para garantizar la existencia de redes seguras consistente en un amplio marco jurídico que logre actuar como factor disuasivo a los ataques a dichas redes, además de poder individualizarlos y procesar judicialmente a quienes los causen.

El objetivo del presente documento, es proporcionar una visión más clara de los componentes necesarios para generar leyes efectivas que sirvan para disuadir y sancionar los ataques a las redes informáticas y a las computadoras, a efecto de ilustrar los conceptos tratados se hace referencia a conceptos básicos del tema, avances del derecho frente a la tecnología, varias normas legales que se hallan vigentes en diferentes estados de nuestro país en materia de delincuencia cibernética; esto con el objeto de establecer normas necesarias que ayuden a crear un marco jurídico efectivo.

Claro está que no es una tarea fácil, el desarrollar marcos jurídicos que vayan más allá con el fin de lograr una protección más amplia de las redes informáticas y de computación, ya que recordemos que dentro de este tema, estamos frente a un ente virtual, el cual puede estar en cualquier parte del mundo, lo cual le facilita la realización de este tipo de delitos.

Tengamos en cuenta que estamos dentro de una amenaza constante, ya que este tipo de delincuentes, son personas decididas, listas, con conocimiento de la tecnología, dispuestas a aceptar retos y con cierto estatus socioeconómico, por tal razón no nos enfrentamos a cualquier delincuente, debido a sus características se les denomina, “delincuentes de cuello blanco”, y los cuales se escudan dentro de las conductas no tipificadas por la ley como delitos para cometer sus ilícitos.

Los daños cometidos por estos delincuentes es incalculable, es difícil identificarlos ya que estos no utilizan la violencia para cometer sus ilícitos, al contrario pueden ser personas respetables por la sociedad, compañeros de trabajo, familiares o amigos, que sin saberlo nosotros, estén ocasionando daños a la economía de un país, atacando a los sistemas de gobierno con el fin de desestabilizarlo, como a sucedido en diversas ocasiones en nuestro país con la página de la Presidencia de la República, Cámara de Diputados, etcétera.

Por esto es de suma importancia que todos actuemos para lograr la actualización o creación de una legislación que nos ayude a tipificar todas estas conductas ilícitas y así se logre crear un frente que disuada y sancione todas estas acciones.

Sabemos de antemano que la tecnología avanza a pasos agigantados, pero no debemos permitir que los delincuentes aprovechen esta situación para cometer ilícitos al amparo de las lagunas jurídicas.

El derecho y la tecnología deben de ir de la mano, no debemos permitir que la tecnología se encuentre en un paraíso que ampare conductas delictivas, por esto, los delitos informáticos constituyen un gran reto para todos los sectores de nuestro país.

CAPITULO I

ELEMENTOS BÁSICOS PARA EL ESTUDIO DEL DERECHO INFORMÁTICO

1.1. Concepto de cibernética e informática

El encuentro de las nuevas tecnologías de la información y comunicación, con el mundo jurídico es inevitable, lo que hace necesario el manejo y la familiarización de una nueva terminología que ayude a comprender el estudio de la materia; por ello es menester definir cibernética e informática.

Cibernética tiene su origen en la voz griega Kibernetes, “piloto” y kybernes, aludiendo al arte de gobernar, así como a la función del cerebro con respecto a la máquina. El estadounidense Norbert Wiener, en 1948, dentro de su obra titulada “Cibernética” la denominó como la nueva ciencia de la comunicación y control entre el hombre y la máquina, asimismo Beer Stafford, la define como: “la ciencia de la comunicación y el control”.

Podemos definir que cibernética, “es la ciencia de la comunicación y el control. Los aspectos aplicados de esta disciplina están relacionados con cualquier campo de estudio. Sus aspectos formales estudian una teoría general del control, la cual tiene aplicación en diversos campos y se adapta a todos ellos” (Téllez Valdés, 2006, p. 3).

Por lo anterior, concluimos que la cibernética es la ciencia de la comunicación y control entre el hombre y la máquina que puede aplicarse a cualquier campo de estudio.

Por lo que respecta a la informática, ésta surge de la misma necesidad de información, para una adecuada toma de decisiones; siendo ésta una palabra nueva, derivada de las palabras información y automatización según Phillipe Dreyfus en 1962.

En sentido General la informática se define como “un conjunto de técnicas destinadas al tratamiento lógico y automatizado de la información para una adecuada toma de decisiones” (Téllez Valdés, 2006, p. 3).

Dicho lo anterior podemos decir que la informática es un conjunto de técnicas destinadas al tratamiento lógico y automatizado de la información para una adecuada, toma de decisiones.

1.2. ¿Qué es una Computadora?

No hay duda que una computadora es una herramienta muy útil en la solución de problemas, lo relevante de esto es su velocidad, ya que el tiempo requerido para que una computadora ejecute una operación varía en microsegundos (millonésimas de segundos) es así como estos aparatos pueden realizar varias operaciones en tan solo unos segundos, trabajando por horas; días ininterrumpidamente sin cometer errores, ya que en su estructura cuentan con la capacidad de comprobar sus operaciones internas, almacenando gran cantidad de información, lo que permite hacer operaciones de cálculos complejos; en resumen podemos enumerar las características de una computadora como sigue:

- Capacidad de almacenar instrucciones e información.
- Gran rapidez y exactitud en la ejecución de instrucciones y cálculos.
- Capacidad de comparar letras o números y decidir una acción.

Esta tercer característica es la que diferencia a una simple calculadora de una computadora, a esto se le llama programa y se denomina como el conjunto de instrucciones programadas por humanos para dirigir a la computadora y que ésta funcione de manera que produzca el resultado deseado, siendo que la computadora

puede diseñar o configurar para satisfacer las necesidades de cada persona, es por esto que una computadora puede ser muy versátil y proporcionarnos gran cantidad de resultados simultáneamente.

Por lo anterior se define a la computadora como “una máquina capaz de procesar gran cantidad de datos, con base en unas instrucciones previas y en tiempo muy corto. Es una herramienta que ayuda al ser humano a simplificar su trabajo” (Vasconcelos Santillán, 1999, p. 322).

Es decir, que la computadora es una máquina electrónica que permite el tratamiento o procesamiento de datos, o más sencillo es una simple caja negra a la cual se le considera así por quedar oculto el procesamiento al que se le alimenta con datos, los cuales son procesados mediante programas y emite un resultado.

1.2.1. Antecedentes de la computadora

Al estar ya familiarizados con el tema de la informática, podemos comenzar a hablar de la computadora; remontémonos a la época de la aparición del hombre cuando tuvo la necesidad de cuantificar los objetos que poseía y empezó a utilizar los medios que tenía a su alcance, como lo eran sus dedos, piedras, trozos de madera, etcétera. La computadora tiene como objetivo computar o procesar datos y eso era lo que precisamente se necesitaba.

Los primeros artefactos utilizados por el hombre, para calcular que se conocen “es el ábaco, utilizado inicialmente en Babilonia o en China y el quipu durante el imperio Inca, consistente en una cuerda, en la que amarraban lazos de diferentes colores, y en estos últimos se hacían algunos nudos” (Vasconcelos Santillán, 1999, p. 35).

Posteriormente es a principios del siglo XIX, cuando surge en el mundo industrial la necesidad de acelerar los cálculos matemáticos, creciendo la actividad económica a un

ritmo que era incalculable, y en el cual se empleaba, a una gran cantidad de personas para calcular y registrar las numerosas operaciones comerciales llevadas a cabo por empresas y bancos; los científicos e ingenieros de esa época al ver la necesidad que se tenía, idearon nuevos modelos de máquinas calculadoras, que día a día iban superando a las otras, resolviendo problemas específicos de negocios.

Es así que llegamos al siglo XX donde se dan los grandes descubrimientos, que permitieron la creación de esas asombrosas máquinas que ya se pueden considerar como una computadora digital, con capacidad para recibir datos mediante un dispositivo de entrada, almacenarlos en la localidad de memoria, procesarlos, ordenarlos, hacer los cálculos necesarios y entregar los resultados con información visual o impresa.

1.2.2. Generaciones de computadoras

En los primeros años del siglo XX, el avance de la tecnología ha sido sorprendente por el descubrimiento de nuevos dispositivos electrónicos, el gran avance de la programación y el desarrollo de sistemas operativos nuevos que ha permitido clasificar a las computadoras de acuerdo a su capacidad de procesamiento en generaciones.

La primera generación se “caracterizó por estar integrada de relevadores (reles) electromecánicos, como la Mark I o de tubos de vació como la ENIAC, eran de un tamaño tan grande que ocupaban espaciosos salones en las universidades donde fueron construidas” (Ferreira Cortes, 2006, p. 28).

Por eso se les denominó como macrocomputadoras y su capacidad de almacenamiento era muy poca, consumían gran cantidad de energía por el número de condensadores, resistencias y válvulas de vacío que tenían y por calentarse demasiado se tuvo que colocar grandes sistemas de refrigeración, su lenguaje era binario, su costo muy elevado, es por eso que IBM la retiró temporalmente.

En la segunda generación “la característica principal es la inclusión de transistores. Siguen dominando los sistemas de tarjetas o cintas perforadas para la entrada de datos” (Ferreira Cortes, 2006, p. 28).

En esta generación se dan grandes logros por lo que toca a la programación, ya que aparecen los primeros lenguajes de alto nivel por ejemplo: Fortran, Algol y Cobol, éste último fue uno de los primeros lenguajes administrativos.

“La tercera generación fue la integración a gran escala de transistores en microcircuitos llamados procesadores o circuitos integrados monolíticos, así como la proliferación de lenguajes de alto nivel y la introducción de programas para facilitar el control y la comunicación entre el usuario y la computadora, así como programas denominados Sistemas Operativos, los cuales facilitan el control y la comunicación entre el usuario y la computadora, es cuando la compañía IBM presenta la primer minicomputadora, la IBM 360 causando gran admiración y fabricándose más de 30,000 de estas computadoras. Es en esta época cuando se empiezan a utilizar medios magnéticos de almacenamiento, como cintas magnéticas y enormes discos” (Ferreira Cortes, 2006, p 30).

La cuarta generación es marcada claramente “por la aparición del primer microprocesador o chip, producido por la compañía Intel Corporation; que era una pequeña compañía de semiconductores ubicada en Silicón Valley” (Ferreira Cortes, 2006, p. 31).

Esta generación se caracteriza por que en un tiempo muy corto alcanzó grandes avances tecnológicos, así como también la aparición de las primeras microcomputadoras, mejor conocidas como computadoras personales, las cuales eran muy sencillas ya que solo se requería de un televisor, una grabadora común de cassettes y el sencillo lenguaje de programación Basic, es por esto la popularidad que adquirió el equipo, ya que no se necesitaba tener grandes conocimientos.

Es en esta generación en la que IBM incluye un Sistema Operativo estandarizado, el cual fue diseñado por el polémico Bill Gates.

La quinta generación es difícil de identificar, ya que muchos autores indican que al no haber cambiado la tecnología de los microprocesadores, se puede seguir considerando que seguimos en la cuarta generación, otros indican que ya la cuarta y quinta generación han terminado, según ellos por el desarrollo de los avances tecnológicos, la verdad es que seguimos avanzando cada vez más y las próximas computadoras tendrán capacidades superiores a las actuales, lo cual ya lo podemos ver con el desarrollo de la inteligencia artificial, reconocimiento de la voz humana, de patrones visuales, razonamiento matemático y aprendizaje de nuevos conceptos.

1.2.3. Elementos de una computadora

La computadora en su nivel estructural se conforma por dos partes “la parte física (que se puede tocar) también llamada hardware, que es el equipo propiamente, y la parte lógica (que no se puede tocar) o software, que son programas y demás instrucciones que necesita la máquina para operar” (Villalobos, 1991, p. 46).

El Hardware lo conforman las partes mecánicas, electromecánicas y electrónicas, así como la estructura física de la misma computadora, la cual se encarga de captar la información, así como la obtención de resultados, en pocas palabras se está hablando de lo que conforma el equipo.

El Software es lo más importante es decir, lo que permite que la computadora ejecute sus actividades, a través de programas

Es por esto que se define a la computadora como una máquina automatizada de propósitos generales, integrada por elementos de entrada, procesador central, dispositivos de almacenamiento y elementos de salida.

Los elementos de entrada los definimos como aquellos elementos que proporcionan o alimentan a la computadora de información, por medio de instrucciones que realiza el equipo periférico, lo que son pantallas, cintas, discos, disquetes, memorias usb, entre otros.

El procesador central, no es más que la unidad central de proceso, mejor conocida por sus siglas en ingles como CPU y es donde se llevan a cabo todas las operaciones lógico matemáticas y su velocidad se mide en gigahertz.

Los dispositivos de almacenamiento como su nombre lo indica son los que contienen o almacenan la información a procesar, su velocidad se puede medir en gigabytes, pero ya por el avance de la tecnología será en terabytes.

Los elementos de salida son aquellos que reciben los resultados del proceso efectuado como lo son las pantallas, impresoras, etcétera.

1.2.4. Lenguajes de programación

El ser humano para comunicarse con los demás tiene que hacerlo por algún medio ya sea oral o escrito y si al comunicarse no se tiene el mismo lenguaje, esto se vuelve muy difícil o imposible, lo mismo pasa con la computadora, el ser humano para poder comunicarse con la computadora debe emplear un sistema de comunicación que le permita la interacción entre el hombre y la máquina, siendo éste el denominado como análogo.

“El lenguaje de programación es el conjunto de palabras, símbolos e instrucciones, que se manejan mediante un conjunto de reglas conocidas por sintaxis y permite descubrir cálculos, toma de decisiones y otras operaciones que debe de realizar la computadora”(Villalobos ,1991, p. 54).

Los lenguajes de programación a través del tiempo han evolucionado notablemente con sus ventajas y desventajas, pudiéndose dividir por su nivel y por sus aplicaciones principales.

Por su nivel, podemos decir que es cuando se refiere a que tan cercanos están los lenguajes a las características de la computadora o que tan cercanos están a las necesidades y por la aplicación se refiere a las ventajas que tiene el lenguaje para resolver problemas.

Los lenguajes de bajo nivel “son aquellos que el procesador de la computadora entiende en forma directa. Dependen de las características de cada tipo de máquina y solo son comprensibles por especialistas. Aparecieron durante la primera generación de computadoras y entran en esta categoría el Lenguaje máquina y el lenguaje ensamblador” (Vasconcelos Santillán, 1999, p. 105).

Es decir son aquellos que dependen de las particularidades de la máquina y son como su nombre lo indica, solo para personas específicas.

Los lenguajes de alto nivel “son aquéllos desarrollados para el usuario de la computadora, permiten que los procedimientos se expresen con un estilo comprensible; sin embargo, la computadora no los entiende directamente” (Vasconcelos Santillán, 1999, p. 105).

Es decir que son para cualquier usuario de computadoras y sus procedimientos son comprensibles, solo que estos deben ser aplicados con ayuda del usuario para que la máquina los comprenda, estos se crearon durante la segunda generación de computadoras; lenguajes de este nivel son Pascal, Basic, Ada.

Algunos autores manejan un tercer lenguaje de nivel medio el cual reúne características de los dos niveles anteriores, un ejemplo de estos son el lenguaje de C.

1.3. Impacto de las computadoras en la sociedad

El desarrollo tecnológico del hombre ha llevado muchos años, sin embargo, en el siglo XX todo ha cambiado, ya que en unos cuantos años los inventos informáticos han alcanzado un gran nivel, esto ha hecho que en la sociedad se genere una forma de pensar distinta, al tener herramientas como la computadora.

Recordemos que después de la revolución industrial se generaron muchos cambios y fue el momento en el que aparecieron sorprendentes inventos como el teléfono, la bombilla eléctrica, la cámara fotográfica, la máquina de escribir, el fonógrafo entre otros, todo esto generó la necesidad de inventar novedosas máquinas que permitieran automatizar todas las operaciones repetitivas y simplificar los cálculos matemáticos.

Tanta fue la necesidad, que después de su aparición, la computadora ha conquistado un lugar de privilegio ante todas las actividades del ser humano, convirtiéndose la informática en parte indispensable en casi todas las actividades de éste, aunado a esto encontramos también los bajos costos de los equipos, los cuales cada vez son más pequeños y en la actualidad la accesibilidad que se tiene para conectarse a la gran red internacional denominada Internet, en la que ya se pueden hacer compras, tener contacto con amigos y familiares que se encuentren lejos, vía correo o chat, así como video conferencias en tiempo real y con tan solo agregar a nuestra computadora una cámara y un micrófono.

En la actualidad los cambios se dan muy rápido y tenemos que adecuarnos a las nuevas tecnologías, no está muy lejos el día en que ya podamos trabajar desde la casa o que los niños ya no tengan que salir de su hogar para tomar clases, ésta es una realidad que poco a poco nos alcanza y que va formando una cultura informática, la cual está creando nuevos esquemas sociales, es por esto que existe la necesidad de crear leyes adecuadas a nuestra actual realidad informática, así como también la forma de relacionarnos con los demás por medio de la red, esto hace que surja la necesidad

de crear una norma ética que regule el comportamiento y las relaciones humanas para no hacer mal uso de esta avanzada tecnología, es aquí donde se reinventan o se complementan las nuevas reglas del comportamiento de la sociedad, que permitan un desarrollo armónico de la humanidad.

Lo anterior obedece a la necesidad de sancionar a aquellos que no respeten las reglas como por ejemplo los hackers y crackers, quienes buscan demostrar su superioridad causando destrozos y robando información para posteriormente hacer mal uso de ella.

Por tal razón, es necesario cumplir y obligar a cumplir las normas establecidas, ya que es una gran responsabilidad de todas aquellas personas que trabajan con una computadora, respetar los ordenamientos legales, por el bienestar de toda la sociedad.

1.4. ¿Qué son las redes y sus antecedentes?

Comenzaremos definiendo que es una red: “esta es un grupo de computadoras y periféricos conectados físicamente y un vasto grupo de programas especializados para permitir el intercambio de datos y compartir los recursos instalados” (Vasconcelos Santillán, 1999, p. 307).

Una red es un conjunto de tecnologías que al interconectarse permiten que muchos usuarios puedan acceder a datos y programas compartidos en tiempo real, estas redes necesitan de hardware y software para interconectar sistemas de cómputo, beneficiando a todos los usuarios al estar compartiendo programas y para las empresas restar costos de operación.

Al aparecer las computadoras personales, se crea la necesidad de conexión de otras computadoras, para el uso y manejo de datos entre ellas, solo que tanto los

programas como equipos no contaban con esta tecnología, es de ahí que surge la necesidad de crear programas útiles que ayudaran a interconectarse entre si.

A medida que las computadoras se iban extendiendo, se comenzaron a ofrecer programas que cubrían con esta característica, lo que desató un gran interés entre la industria y organizaciones, por la importancia de la comunicación entre computadoras y la transferencia electrónica de información, esto ha originado la creación de redes de capacidad cada vez más grandes y de mayor velocidad.

Las redes cuentan con distintas formas, no es el típico salón con un número de computadoras conectadas entre si y compartiendo la impresora, es algo más complicado y para darnos idea de esto, la red puede incluir todas las computadoras y dispositivos de una compañía, de una ciudad y hasta de un país, esto nos hace imaginar si se conectaran diversas redes individuales en una red masiva, todos los que estén conectados podrían intercambiar una gran cantidad de información; siendo Internet la red más grande que existe actualmente.

Es por eso que en términos técnicos, Internet es “un conjunto de elementos tecnológicos que permiten la interconexión de redes de diferentes tipos; de este modo los datos que se localizan en una red pueden ser aprovechados por otra” (Vasconcelos Santillán, 1999, p. 308).

“Internet en la actualidad realiza la interconexión de redes a nivel mundial es por eso que Internet es en realidad una “red de redes” y no solo una red de tamaño mundial; para distinguir cada red, estas tienen su propia dirección o nombre, las direcciones constan de una secuencia numérica que suele tener asociado un nombre, entonces se puede decir que la dirección completa de una computadora consta de una dirección dentro de la red y de la dirección de la red” (Vasconcelos Santillán, 1999, p. 308).

Internet comienza a finales de los años setenta en Estados Unidos, con propósitos militares, como casi todos los avances tecnológicos, este sistema de comunicación se creo con el fin de tener una red de comunicación mas efectiva y confiable; es por su efectividad que el departamento de Defensa de los Estados Unidos, en el año 1990 crea el sistema de Internet.

Este sistema es también compartido con universidades de los Estados Unidos, siendo la Universidad de Texas en San Antonio, EUA, la primera que en el año de 1989 realiza la primera conexión de este tipo en nuestro país, con el Instituto Tecnológico y de Estudios Superiores de Monterrey, Nuevo León.

Es entonces que en 1990, Internet viene a revolucionar los medios de comunicación, ya que permite a cualquier persona poder comunicarse desde cualquier parte del mundo, en nuestro país este avance llega en el año 1993.

Para poder enlazarse a Internet, es necesario comunicarse con un servidor que permita el acceso vía modem (este es un dispositivo que se encarga de convertir datos binarios en señales eléctricas); y que éste a su vez se encargue de las transferencias con otras redes, otra forma sería si no se cuenta con acceso a la red, por medio de una línea telefónica.

Las principales aplicaciones con las que se cuentan dentro de Internet son:

Correo electrónico: este permite “la comunicación con otras personas, se realiza con el correo electrónico (e-mail). Este servicio permite el intercambio de mensajes entre dos usuarios sin necesidad de que ambos estén presentes al mismo tiempo, mediante Internet se vuelve posible la comunicación con personas de diferentes países del mundo” (Vasconcelos Santillán, 1999, p. 308).

Transferencia de archivos: este permite que cualquier persona pueda tener a su alcance cualquier archivo no importando en donde se encuentre ya que mediante este sistema se pueden tener datos o información sobre temas particulares.

Acceso remoto: éste consiste en poder controlar una computadora que se encuentra situada en otro país, siempre y cuando se encuentre conectada a Internet y poder tener información a la mano desde distancias remotas.

Con esto podemos ver el importante papel que juega la red de computadoras, la cual va creciendo cada día más y abre una diversidad de posibilidades, ya que no es solo un medio de comunicación, sino también nos da la oportunidad de tener contacto con más personas, compartir opiniones y conocimientos. De ahí la importancia de una regulación eficaz y efectiva que controle todo este mundo informático.

1.4.1. Riesgos en la red

Después de ver todas las ventajas que las redes tienen, es importante saber que existe un peligro latente al usar la red, esto parecerá ser exagerado pero el hecho de tener una computadora con acceso a Internet, abre la puerta y facilita la acción de los virus y piratas informáticos, ya que estas conexiones se mantienen abiertas y es seguro que los piratas ya hayan encontrado un sistema y determinado si pueden invadir una computadora, esto es más sencillo con las computadoras domésticas, ya que éstas tienen, por el tipo de programas, fallas en los sistemas de seguridad, así como problemas con las contraseñas que los usuarios utilizan en su sistema.

Los piratas o intrusos se mantienen recorriendo Internet, tratando de identificar computadoras a las que puedan acceder, contando con herramientas de software que les facilite el trabajo, el primer paso de la invasión consiste en activar un comando denominado “ping”, el cual se dirige hacia su computadora, ésta a su vez informa si está encendida y conectada a Internet, posteriormente el invasor busca la forma de

acceder al sistema de la computadora, una vez dentro comienza el daño, los archivos con datos importantes pueden ser renombrados, desplazados, eliminados o copiados, así como también utilizar la computadora para sus fines sin que nos demos cuenta.

1.4.2. ¿Cómo surgen los virus informáticos?

Los virus surgieron a finales de 1990 y han protagonizado grandes noticias, debido a su capacidad de ocasionar daños y trastornos, estos virus están diseñados para esconderse, ocasionar daños y no ser detectados por el mayor tiempo posible, sin embargo, el daño que provocan los virus han ocasionado grandes pérdidas de datos y productividad, cobrando cada vez más fuerza y convirtiéndose en más exitosos cuando el usuario no está consiente del riesgo que corre su equipo y tampoco toma las medidas de seguridad necesarias para protegerlo.

Los virus se pueden prevenir, siempre y cuando se cuente con algunos conocimientos y herramientas de software, estos virus pueden provenir de diversos lugares como lo son el correo electrónico, un CD o disco, así como también se ha comprobado que en ocasiones al comprar un programa de computadora que se adquiere en tiendas, han contenido virus, por eso es muy importante que se tenga un software antivirus, con el fin de que mantenga nuestro equipo libre de virus y erradicarlos.

Existe un inconveniente con respecto a los software antivirus y esto es que ninguno te da una protección completa, ya que van surgiendo cada vez nuevos virus, es por eso que algunas compañías de antivirus permiten que los usuarios descarguen bases de datos de información y el código que puede erradicar a los virus, esto es mejor conocido como vacunas, por eso es recomendable que por lo menos cada semana se compruebe la efectividad del antivirus y revisar las últimas actualizaciones con el fin de tener protegido nuestro equipo.

1.4.3. ¿Qué es un Virus?

“Es un programa parasitario que infecta a un programa legítimo el cual se conoce como el anfitrión; para infectar el programa anfitrión, el virus modifica al anfitrión para almacenar una copia del virus” (Norton, 2006, p. 578).

Una vez que se ha infectado el sistema de la víctima el virus está listo para hacer daño, los virus están diseñados para hacer distintos tipos de daños y este daño que provoca no es lo que lo define.

Por lo anterior, podemos decir que los virus son pequeños programas que dañan o borran información que contiene una computadora, se les llama así por que se adquieren de contagios similares a los biológicos.

Para que un virus lo sea, necesita tener la capacidad de replicarse o copiarse a si mismo, en distintos lugares de la computadora o buscar la forma de llegar a otras computadoras por ejemplo, en la red o en discos infectados, siendo ésta primera la forma más usual de propagación del virus, así como salones de charlas, de mensajería instantánea.

Los virus benignos no causan tanto daño, su propósito es solo molestar al usuario y no causan un daño específico; en cambio existen otros que son todo lo contrario y si pueden ocasionar diversos daños graves si se les permite ejecutarse.

Existe un programa llamado Caballo de Troya cuyo principal objetivo es el de “abrir una puerta trasera en el sistema infectado, lo cual permite que otra persona acceda e incluso tome control del sistema a través de una red o conexión de Internet” (Norton, 2006, p. 579).

Esto es que otra persona entra a la computadora y toma el control del sistema a través de la red, este tipo de programas son utilizados para convertir un sistema infectado en un zombi, que es utilizado para poder atacar a otros sistemas, este tipo de ataque se le llama denegación de servicio, ya que consiste en que el autor del virus crea una cantidad de sistemas zombi y así utilizarlos para enviar miles de solicitudes a un servidor haciendo que éste se sature y no proporcione servicio a los usuarios.

Lo virus son un problema para todos nosotros, pero para las empresas representa un golpe devastador, debido a la pérdida de información, productividad y recursos que se invierten en la localización y eliminación de los virus, así como las pérdidas millonarias que por los daños ocasionados a los sistemas se den.

1.4.4. Principales virus informáticos

¿Qué pasa cuando escuchamos la palabra virus?, es una palabra que nos coloca en un estado de alerta, aunque como ya se mencionó la mayoría de estos no causan gran daño sino molestia, sin embargo, trataremos de describir algunas de las categorías de virus, gusanos o programas de ataque de tipo Caballo de Troya, ya que estos programas representan la amenaza más común a la información.

“Los virus de grupo realizan cambios al sistema de archivos de un disco, esto es que si algún programa infectado del disco es abierto, el programa hace que el virus también se ejecute, creando la ilusión de que el virus ha infectado a todos los programas del disco” (Norton, 2006, p. 580).

“Existen otros tipos de virus llamados virus bimodales, bipartitas o multipartitas. Estos tipos de virus pueden infectar archivos y también el sector de inicio del disco, este tipo de virus es muy molesto ya que lo que ocasiona es que la máquina queda completamente inaccesible hasta que se elimine el virus” (Norton, 2006, p. 580).

Las bombas lógicas es otro tipo de virus, aunque algunos autores no lo consideran así, no obstante se les tiene que denominar como virus, ya que de igual forma ataca ocasionando daños o trastornos a un sistema, éste es un programa de rutinas o modificaciones, que borra o realiza alteraciones al sistema, este programa no actúa en el momento, es decir, actúa hasta que se produzca una determinada operación o código para ejecutarse, sus características son:

- Su ejecución es retardada.
- El creador sabe cual es el daño que causa y cuando se ejecuta.
- La operación de ejecución es determinada por el creador.
- Este código no se replica.
- Los creadores casi siempre suelen ser personal de alguna empresa o institución que no están de acuerdo con políticas y suelen programar este virus para realizar el daño.

Los virus del sector de inicio, se consideran de los más hostiles, ya que infectan el sector de inicio de un disco, ya sea duro o flexible, removiendo el sector de inicio, parte importante para que una computadora pueda dar inicio. Este virus al ejecutarse se copia a si mismo y se guarda en la memoria de la computadora, para así poder infectar otros discos.

“Virus de correo electrónico, se transmiten a través de mensajes, no importando si es en redes privadas o por Internet, algunos de estos virus se transmiten como un archivo adjunto, ya sea un documento o un programa, que se adjunte al mensaje, y es ejecutado cuando la víctima abre el archivo que está adjuntado al mensaje, otro tipo de virus de esta categoría se encuentra dentro del cuerpo del mismo mensaje, solo que

para que el virus se adjunte al mensaje es necesario codificarlo en formato HTML, este virus una vez ejecutado se propaga por todas partes enviando mensajes a todas las personas que se encuentran en la libreta de direcciones de la víctima, conteniendo en cada mensaje una copia del virus, haciendo la misma tarea al llegar a su objetivo" (Norton, 2006, p. 580).

También existe un tipo de virus que solo ataca a un determinado tipo de programas, este se llama virus de macro, por ejemplo, solo archivos de Excel o Word, ya que estos programas pueden contener macros, estos macros son programas pequeños que se utilizan normalmente para emitir comandos de programa específicos, pero que también pueden emitir ciertos comandos del sistema operativo. El virus de macro se incrusta en un archivo de documento como si fuera un macro, creando distintos niveles de daño a los datos desde la descomposición de documentos hasta la eliminación de datos.

Los virus que infectan archivos es otro tipo de virus, éste infecta a los archivos de programa de un disco, actuando al iniciar un programa infectado, ejecutando el código de virus.

Existen otros virus que se les llama polimorfos, autotransformables, autocifrables o autocambiantes, este tipo de virus tienen la característica como su nombre lo dice, de ir cambiando a si mismos cada vez que se copia, lo cual hace difícil identificarlos y ubicarlos para su destrucción.

"Los programas de broma, no son virus ni tampoco ocasionan daño, su propósito real es el de asustar a la víctima haciéndola creer que efectivamente el virus ya se encuentra dentro de su computadora infectando y dañando su sistema, alertando a la víctima que no debe tocar ninguna tecla o el virus será ejecutado formateando el disco duro, por consecuencia perderá toda su información, siendo todo esto una gran mentira" (Norton, 2006, p 580).

“Virus ocultos, estos se alojan dentro de la memoria de la computadora, por tal razón es difícil su detección, también ocultan cambios que hacen a otros archivos, ocultando daños al sistema operativo y al usuario” (Norton, 2006, p. 580).

El virus llamado Caballo de Troya, técnicamente no es un virus, debido a que no se duplica asimismo en el disco de la víctima, o en otros discos, pero se le considera virus debido al daño que causa, este programa como su nombre lo dice es un programa que aparenta ser amigable, siendo en realidad un programa malicioso, ocultándose y aparentando ser por ejemplo un juego, sin embargo, este programa es utilizado muy a menudo por los piratas informáticos, para crear las llamadas puertas traseras dentro de las computadoras infectadas para acceder a ellas sin ningún problema.

Los gusanos tampoco se les consideran como virus, solo que como también causan daños considerables se tratan como si lo fueran, estos son programas los cuales tienen el propósito de duplicarse así mismos, para que sea efectivo este programa, el gusano deberá duplicarse hasta llenar discos enteros de copias de si mismo, ocupando todo el espacio libre de la memoria del sistema. Existen otros que están diseñados para hacer todo lo posible para que estos se propaguen a otras máquinas, por ejemplo, un sistema de correo corporativo podrá quedar obstruido con copias de este virus, dejándolo completamente impedido e inútil, estos tipos de virus como ya lo vimos se transportan por medio de mensajes adjuntos por el correo electrónico y canales de chat, vía Internet.

1.5. Antecedentes del derecho informático

El derecho informático, es una rama del derecho que se encuentra en pleno desarrollo, debido a que la informática hoy en día se involucra en todos los campos de la vida moderna, con mayor o menor rapidez en todas las ramas del saber humano, este se rige ante los progresos tecnológicos y comienzan a utilizar los sistemas de información para ejecutar tareas que en otros tiempos se tendrían que realizar manualmente.

El progreso de todos los sistemas computacionales permite poner a disposición de la sociedad una cantidad inimaginable de información de todo tipo, al alcance de todos los usuarios de Internet y la cual es libre y sin limitaciones.

Debido a lo anteriormente expresado, podemos determinar que el derecho y las comunicaciones tienen un estrecho camino y que sin duda se entrelazan debido al control que tiene el hombre sobre las máquinas, ya que caemos en el fenómeno jurídico, y aunque existen tratados de casi medio siglo en los que se explicaba esta relación hecha por visionarios que ya esperaban un avance de la tecnología, nunca llegaron a imaginar los cambios que se están dando en nuestros días.

La rama del derecho informático es reciente y se encuentra en pleno crecimiento, habla de materias totalmente distintas por su naturaleza, según la visión algunas personas, pero que al ir avanzando nos damos cuenta que la tecnología no podrá avanzar sin normas jurídicas que regulen esta actividad, llevándonos al mundo del ser y del deber ser; en el que el ser, denota en que consiste una realidad algo que está, estuvo o estará, y el deber ser estableciendo un comportamiento como debido que debe ser cumplido, aunque es claro que esta disposición puede que no se observe o se vaya a observar.

Las consecuencias con respecto a los delitos informáticos, ya se veían venir desde hacia mucho tiempo y versaban en cuanto al Derecho, posteriormente ya con el estudio de las implicaciones jurídicas, motivadas por la informática comienza la necesidad de un Derecho que estudie todas estas nuevas implicaciones.

1.5.1. Clasificación del derecho informático

El derecho informático se define como “una rama de las ciencias jurídicas que considera a la informática como instrumento (Informática Jurídica) y objeto del estudio (Derecho de la Informática)” (Téllez Valdés, 2004, p. 17).

Como hemos podido ver es un tema difícil de clasificar o conceptuar ya que es un tema en constante cambio, por un gran número de peculiaridades y de opiniones, pero de lo que si debemos estar seguros es de que hoy la informática ocupa una gran parte de los campos de nuestra vida y todas las ramas del saber humano se rinden ante los progresos que representa.

Hoy en día este avance de la informática no solo lo podemos ver por el lado favorable, sino que también plantea problemas de importancia para su funcionamiento y la seguridad del mismo, es por eso que se necesita una regulación que esté lo más actualizada y eso no es tarea fácil.

1.6. Antecedentes de la informática jurídica

“La informática jurídica es una materia que va evolucionando y sufre cambios, a fin de que cada vez se vaya ajustando a los cambios actuales; ya son casi 50 años de la aparición de la informática y fue en el Healt Law Center de la Universidad de Pittsburg, Pensylvania, cuando el entonces director del centro, John Horty, estaba convencido de la necesidad de encontrar medios satisfactorios para tener acceso a la información legal. Para 1959, el centro colocó ordenamientos legales en cintas magnéticas y es aquí cuando se hace uso por primera vez de la informática al servicio de la materia del derecho, ya que se dieron cuenta que no solo servía para fines matemáticos, toda vez que estaban convencidos de que esto podría servir para poder tener acceso a la materia legal, es por esto que se comienza a explorar esta tecnología, dando como resultado un sistema automatizado de búsqueda de información”, (Téllez Valdés, 2006, p. 18).

En nuestros días, ya podemos consultar todo tipo de materias, es más en Internet, los usuarios pueden hacer búsquedas de cualquier tema que les interese y siempre encontrarán información referente al tema que esté consultando.

Podemos decir que la informática, es una materia tan extensa que abarca los fenómenos más significativos en prácticamente todas las áreas del conocimiento, por lo tanto, no se puede excluir a la materia jurídica; debido a esto podemos definir a la informática jurídica en forma general como el conjunto de aplicaciones de la informática en relación con el derecho.

1.6.1. Concepto de informática jurídica

Existen tantas definiciones y tantos autores que han intentado dar una definición lo más acertada a la informática jurídica, pero por ser ésta una materia que se encuentra en expansión es difícil; de lo que si podemos estar seguros es de que se trata del empleo de la computadora en el ámbito jurídico.

“La Informática jurídica se define como la técnica interdisciplinaria que tiene por objeto el estudio e investigación de los conocimientos de la informática general, aplicables a la recuperación de información jurídica, así como la elaboración y aprovechamiento de los instrumentos de análisis y tratamiento de información jurídica necesarios para lograr dicha recuperación, es importante señalar que se define como una técnica que estudia e investiga a la informática, para aplicarla al rescate de información, que sirvan como herramienta de estudio de información jurídica, necesaria para lograr dicha recuperación, la cual es un instrumento vital en nuestros días, no solo por la comodidad sino por la rapidez con la que se puede consultar la información que en otros tiempos hubiera necesitado de un gran número de personas y tiempo, para encontrar dicha información” (Téllez Valdés, 2006, p. 19).

Hoy en día lo podemos observar en cualquier institución de gobierno en universidades, empresas, bancos, etcétera.

El uso de la informática es tan grande y de mucha ayuda que resulta una herramienta indispensable para todas las áreas del conocimiento humano.

1.6.2. Clasificación de informática jurídica

En el campo de la informática, el derecho se encuentra dividido en diferentes formas, por ejemplo, archivos legislativos, bibliográficos, doctrinales, jurisprudenciales, los cuales representan una gran ayuda a la información y facilita en gran manera el trabajo y tomas de decisiones de los abogados, jueces y magistrados, ya que representa una gran ayuda en el mundo del derecho.

La informática jurídica no es solo la herramienta que utilizamos todos los abogados para revisar leyes, jurisprudencia o doctrina, es decir, solo para consultar con más rapidez y exactitud información de interés jurídico; es algo que va más allá al avance de la tecnología, y ha abierto las puertas a nuevos programas que no solo proporcionan información, sino que ya realizan actos jurídicos.

Por lo anterior podemos clasificar a la informática jurídica de la siguiente forma:

- Informática documentaria: ésta se encarga de recopilar y recuperar todos aquellos textos jurídicos.

- Informática jurídica y de control de gestión: ésta se refiere a las actividades jurídicas.

- Informática jurídica meta documentaria: ésta ayuda en todo el marco de redacción, investigación, de toma de decisiones, educación y previsión del derecho.

Existen muchos juristas que hasta la fecha se mantienen en actitud de escepticismo ya que comentan que aunque la informática jurídica permita un mejor conocimiento de los fenómenos jurídicos, no creen que la computadora sea un instrumento tan eficaz a prueba de errores. Algunos otros opinan todo lo contrario teniendo una visión

completamente distinta y considerando a la computadora como una herramienta efectiva para un mejor desarrollo y desempeño de su labor.

Este tipo de tecnología además de todos los beneficios que aporta, nos ayuda a tomar mejores decisiones en todo el universo jurídico, nos llena de información de una forma rápida y ágil con el fin de tener un mejor conocimiento del tema, esto representa ser un gran avance en todos los sentidos del mundo del derecho.

CAPITULO II

ASPECTOS GENERALES DE LA DELINCUENCIA INFORMÁTICA

2.1. El Derecho ante el avance tecnológico

Es preocupante el hecho de que los avances tecnológicos han abierto nuevas posibilidades de actividades delictivas, en particular la utilización de la tecnología de la información y medios de telecomunicación con fines delictivos, por eso es necesario que se intensifiquen los esfuerzos por combatir de forma más eficaz los abusos relacionados con la informática, recordando que la información promueve el desarrollo económico, social, democrático y de educación de un estado.

Es sabido por todos que dentro de la ley existen lagunas para la utilización de la tecnología de la información, también sabemos que es necesario que los Estados y las empresas privadas, coadyuven para evitar la utilización de la tecnología con fines delictivos, subrayando la necesidad de fomentar la coordinación y cooperación entre los estados, para luchar contra la utilización de la tecnología de la información con fines delictivos.

“Como se ha venido comentando, es necesario regular la actividad informática y su relación con distintos derechos para conceder seguridad jurídica a los usuarios de la red, en el uso y aplicaciones de la tecnología informática” (Molina Salgado, 2003, p. 87).

“Es necesario que las leyes y reglamentos relacionados con la información, estadística y comunicaciones sean reformados para incluir y establecer de forma clara y precisa, conceptos básicos de los medios y las actividades informáticas, incluyendo los derechos y obligaciones de quienes prestan servicio de telecomunicaciones, de quienes operan los sitios de Internet”. (Molina Salgado, 2003, p. 88).

Regulando todas las funciones propias de sus sistemas, así como la forma de almacenar información, procesamiento y transferencia de la información en sus sistemas y sus tecnologías.

Esto será una base para que se regule jurídicamente a la informática y así poder tipificar cada una de las conductas y sancionarlas de acuerdo a su gravedad, esto ayudaría a administrar la actividad informática y su convivencia pacífica con el derecho, ya que a medida de que las autoridades se vean en la necesidad de aplicar criterios y preceptos administrativos o legales para la prevención de delitos, estos ya se encontrarán dentro de lineamientos que los castiguen.

“Sabemos por amargas experiencias, que los medios informáticos alteran, al menos en parte, los esquemas tradicionales de interacción social y ofrecen nuevas formas de relación interpersonal” (Andrés Campoli, 2005, p. 17).

Esto da como consecuencia el hecho de que también sirve como medio de comisión de delitos ya tipificados en las leyes penales, y pueden generar violaciones de bienes jurídicos protegidos, pero que hasta la fecha la vulnerabilidad no se considera como delito, pero con esta actividad por lo menos violan la regla normal de convivencia pacífica en sociedad.

Es razonable que no todas las conductas posibles se deriven en conductas criminalizadas, pero lo que no se puede negar es que algunas de estas nuevas conductas sí deben estar contenidas en los ordenamientos legales.

Debido a estas conductas, podemos hablar entonces que a la actual sociedad de la información, le corresponderá una estructura propia de instituciones que proporcionen, al menos, la seguridad necesaria para el desarrollo normal de la misma (Andrés Campoli, 2005, p. 18).

“Hasta hace todavía pocos años, a la hora de caracterizar a la sociedad en la que vivimos, se utilizaba el adjetivo “postindustrial”. Después sin que se tenga que descartar ese rasgo para aludir a las condiciones de la vida contemporánea, han aparecido otras expresiones que se usan preferentemente. Entre ellas ocupa un lugar destacado la de “sociedad de la información”. (Recuperado 2 de junio de 2007 de http://www.ejournal.unam.mex/boletin_mderecho/Bolmex109/BMD10903.pdf)

Estas denominaciones pretenden poner de manifiesto que como consecuencia de los avances tecnológicos y de los cambios culturales que se han ido produciendo, las relaciones sociales contemporáneas se distinguen por el volumen de información que se produce y circula en forma masiva y sistematizada.

Esta sociedad de la información se considera hoy como un fenómeno global y supone un conocimiento integral en el movimiento de informatización de los aspectos históricos, políticos, económicos, culturales, científicos y técnicos, cuyas repercusiones sociales son considerables.

El Derecho en cambio es una parte inseparable en el mundo de la tecnología, ya que por un lado, éste utiliza los beneficios de los avances, y la utilización de estas tecnologías nos facilitan el trabajo, además de ser un apoyo dentro de los procedimientos de los tribunales, en la gestión de los abogados y en la administración pública, todo esto englobado dentro de la informática jurídica.

La intervención del derecho en esta materia se torna urgente, ya que siendo ésta una nueva cultura dentro de la sociedad, deberá existir un conjunto de reglas que rijan en todo caso un gran número de situaciones y de las cuales tenemos: La regulación jurídica de la información, la protección de datos personales, la regulación de Internet, los contratos informáticos, protección de los programas de computación, los delitos informáticos, regulación de los nombres de dominio, comercio electrónico, el teletrabajo, el valor de la firma digital y electrónica.

En el mundo en el que vivimos, en nuestro entorno inmediato, el impacto tecnológico es tan intenso y acelerado que nos condiciona decisivamente y hace que cambien cada vez más las coordenadas en las que nos movemos. Así, ahora se ha empezado ha utilizar la expresión sociedad red. (Recuperado 2 de junio de 2007 de http://www.ejournal.unam.mex/boletin_mderecho/Bolmex109/BMD10903.pdf)

Esta sociedad es una forma de vida asociada caracterizada por dinamismo y complejidad, así como por la descentralización, naturalmente todo esto trae consecuencias muy importantes sobre todo en el plano de las relaciones sociales, y no todas son positivas, pues la tecnología, al tiempo que da seguridad a algunos, trae inseguridad a muchos más.

Hemos llegado a un punto en el que las barreras físicas y temporales, que impedían o dificultaban la comunicación e información han quedado atrás.

2.2. Orígenes del delito informático

Como ya lo mencionamos, “las redes de comunicación y los sistemas de información forman parte integrante de la vida diaria de los ciudadanos del mundo y desempeñan un papel fundamental en el éxito de la vida económica de un país y del mundo” (Téllez Valdés, 2004, p. 162)

Cada vez son más las conexiones a la red, lo que implica una mejor y mayor ventaja, pero también conllevan a un gran riesgo de ataques mal intencionados a los sistemas de información, estos ataques pueden ser de distintos tipos; desde el acceso ilegal hasta la contaminación de redes por programas dañinos, lanzando los ataques desde cualquier lugar del mundo, produciéndose un retroceso dentro de la economía de un país a raíz de estos ataques.

Debido a lo anterior podemos decir que estamos frente al delito informático, el cual es la conducta cuya realización afecta un nuevo interés social ligado al tratamiento de la información. (Recuperado 2 de junio de 2007 de http://www.monografias.com/trabajos23/bien-juridico/bien-juridico.shtml#delitos)

“Los delitos informáticos comienzan a darse después del surgimiento de los medios informáticos, a mediados del siglo XX, estos primeros actos ilícitos no fueron cometidos intencionalmente, si no que fueron a raíz de errores o descuidos”. (Molina Salgado, 2003, p. 17).

Además de que la era tecnología que apenas surgía, ya posteriormente al considerar todos estos elementos, comienza a surgir la mala fe y el dolo, dando inicio así a la proliferación de los delitos informáticos.

El delito informático es un término muy amplio referido a los problemas que aumentaron el poder informático, abarataron a las comunicaciones y provocaron que haya surgido el fenómeno de Internet para las agencias policiales y de inteligencia. (Recuperado 2 de junio de 2007 de http://www.vecam.org/article659.html)

Los hackers, crackers y ciberpiratas, son aquellos que vienen a romper con el esquema de la tecnología, “ya que recordemos que a toda tesis corresponde una antítesis”, (Molina Salgado, 2003, p. 17).

Esto mismo se aplica a la tecnología, creando una antitecnológica informática, superando los alcances y capacidades de la tecnología informática, es decir, que desde los primeros días de la tecnología, siempre existió alguien que buscara la forma de modificar, destruir e impedir el acceso a la información a otros usuarios, a través de virus y otros métodos.

“Hacker, es un término empleado para identificar indistintamente a un programador habilidoso, o bien, a un allanador de sistemas informáticos que altera programas” (Molina Salgado, 2003, p. 17).

“Cracker, proviene de crak que significa romper algo o descifrar un código y sirve para identificar a quienes entran simplemente en sistemas informáticos de terceros constantemente” (Molina Salgado, 2003, p. 17).

“Ciberpiratas, son aquellos que roban propiedades de terceros en la red para después extorsionar a los legítimos titulares o venderlos al mejor postor” (Molina Salgado, 2003, p. 17).

Es así que con la aparición del medio informático llamado Internet, que estuvo a disposición del público en general, los ciberpiratas comenzaron a aparecer, moviéndose en un medio que les beneficiaba para cometer conductas delictivas sin ser detectados; de estas actividades ilícitas es de donde surge lo que hoy conocemos como delitos informáticos.

En un principio el delito informático, se aplicaba a nuevos tipos de criminalidad, tales como la pornografía cibernética, o la distribución de imágenes, que violaban algunas pero no todas las leyes de los países con respecto a la pornografía inaceptable o al material utilizado para explotar. (Recuperado 2 de junio de 2007 de http://www.vecam.org/article659.html)

El hecho de que Internet no tenga fronteras facilita a las personas a cometer ilícitos, sin mostrar su rostro, al igual que la piratería, es por eso la importancia de luchar contra esta nueva actividad delictiva.

Sin duda los delitos informáticos a través de su estudio y el avance del tiempo, encontrarán una concientización dentro de todos los miembros de la sociedad.

2.2.1. Elementos del delito informático

En el Congreso Sobre Redacción de Legislación en Materia de Delitos Cibernéticos de la OEA (2004 27 de enero), se realizó el análisis de los elementos del delito informático, en el que se estableció que son todos aquellos elementos necesarios para la comisión de la conducta delictiva entre los que se encuentran los siguientes:

- Sistema computacional: todo dispositivo o grupo de dispositivos interconectados o relacionados en el que uno o más de ellos realizan funciones de procesamiento automático de datos.

- Datos computacionales: toda representación de hechos, información o conceptos de forma tal que puedan ser procesados en un sistema computacional, incluyéndose los programas que hagan que dicho sistema desempeñe una función dada.

- Prestador de servicios:

    1. Toda entidad pública o privada que brinde a sus usuarios la posibilidad de comunicarse mediante un sistema computacional.

    2. Cualquier otra entidad que procese o almacene datos computacionales en nombre del mencionado prestador de servicios de comunicación o de los usuarios del mismo.

- Datos de tráfico: Todo dato computarizado relativo a una comunicación por medio de un sistema computacional, generado por un sistema computacional que forma parte de la cadena de comunicación y que indica el origen de ésta, como así también su destino, ruta, hora, fecha, tamaño, duración o tipo de servicio.

2.2.2. Concepto de delito informático

Es difícil dar un concepto exacto que defina lo que es el delito informático, debido a que son conductas antisociales en plena expansión y que debido a su naturaleza es probable que no se puedan considerar como delitos.

Es por eso que podríamos decir que el delito informático es toda acción conciente y voluntaria que provoca un perjuicio a persona natural o jurídica sin que necesariamente conlleve a un beneficio material para su autor, o que por el contrario produce un beneficio ilícito para su autor aun cuando no perjudique de forma directa o inmediata a la víctima, y en cuya comisión interviene indispensablemente de forma activa dispositivos normalmente utilizados en las actividades informáticas. Recuperado 3 de junio de 2007 de http://www.laflecha.net/articulos/seguridad/delito_informatico/

Encontramos otra definición de delito informático que dice son todas aquellas conductas ilícitas susceptibles de ser sancionadas por el derecho penal, que hacen uso indebido de cualquier medio informático. (Recuperado 3 de junio de 2007 de http://www.delitosinformaticos.com/delitos/delitosinformaticos.shtml)

“Por lo que hace al concepto legal, nuestra legislación penal federal no prevé una definición de la expresión delitos informáticos, sin embargo, dicha legislación contempla como delito de carácter informático, el acceso ilícito a sistemas y equipos de informática” (Molina Salgado, 2003, p. 18).

Debido a lo anteriormente expresado, nos damos cuenta que es difícil el poder proporcionar un concepto ya que la denominación alude a una situación fuera de lo ordinario y hasta la fecha en la mayoría de los países no se prevé una definición exacta, cayendo en el supuesto de no abarcar todos los elementos del delito, ya que como se mencionó es una materia que apenas está en plena expansión y requiere de un estudio más profundo.

En el ámbito teórico doctrinario, se define como “actitudes contrarias a los intereses de la persona en que se tiene a las computadoras como instrumento o fin (concepto atípico) o las conductas típicas, antijurídicas y culpables en que se tiene a las computadoras como instrumento o fin (concepto típico)” (Téllez Valdés, 2004, p.163).

De acuerdo con el concepto atípico, los delitos informáticos son actitudes ilícitas en que se tiene a las computadoras como instrumento o fin, por su parte el concepto típico señala que son las conductas típicas antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin.

Con respecto a esta definición de Téllez Valdés, Molina Salgado dice que, “podría mas bien estar relacionado con aquello a lo que nos hemos referido como ilícitos informáticos, los cuales son o pueden ser de una naturaleza muy distinta a un delito, ya que estos pueden constituir actos ilícitos de menor grado como infracciones administrativas y la competencia desleal” (Molina Salgado, 2003, p. 19).

2.2.3. Características del delito informático

Como ya se había mencionado con anterioridad, estos “tipos de delitos son aquellos que poseen ciertas características que no presentan el denominador común de los delincuentes, esto es, los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles con el uso de los sistemas informatizados, aun cuando, en muchos de los casos, no desarrollen labores que faciliten la comisión de este tipo de delitos (Téllez Valdés, 2004, p. 164).

Con el tiempo se ha podido observar que existen diversos grados de delitos debido a su naturaleza por ejemplo, no es lo mismo el que ingresa a una computadora sin intenciones delictivas, que siendo un empleado bancario que traspase fondos de otras

cuentas a la suya, esto nos da una idea también de que en muchas ocasiones los delitos informáticos, son realizados por los mismos empleados y no por personas externas de una institución, este dato lo revelan distintos órganos internacionales.

Es difícil detectar o hacer un perfil de un delincuente informático, ya que por el hecho de que se tengan conocimientos o aptitudes en sistemas informáticos no podemos inferir en delincuencia informática, por lo tanto, podemos tener a una persona que trabaja en una institución privada o de gobierno, que cuenta con diversas características como son decisión, motivación y disposición a aceptar un reto, características que pueden encontrarse en cualquier empleado y no por eso se le puede considerar como delincuente, pero siendo éste el caso de que cometa el ilícito, a estos individuos se les considera como “delincuentes de cuello blanco”.

“El sujeto activo del delito, definido como delincuente de cuello blanco es aquella persona, que cuenta con un determinado estatus socioeconómico, su ilícito no es cometido por pobreza ni por baja educación, poca inteligencia o inestabilidad emocional, todo lo contrario, es el que se siente seguro de cometer sus ilícitos ya que puede estar distribuido en cualquier parte del mundo bajo leyes y jurisdicciones diferentes, por lo tanto, la posibilidad de castigo es limitada” (Téllez Valdés, 2004, p. 164).

“Sus características son:

1. Conducta que solo un número de personas con determinados conocimientos la puede cometer.

2. Es una acción ocupacional ya que en ocasiones se realiza dentro del trabajo.

3. Son acciones de oportunidad creadas e intensificadas.

4. Provocan grandes pérdidas para los afectados.

5. Comodidad de tiempo y espacio ya que para cometer el ilícito no es necesaria la presencia física y solo bastan unos cuantos segundos para cometerlo.

6. Debido a la falta de regulación son pocas las denuncias.

7. Los delitos informáticos son sofisticados.

8. Por su carácter técnico resulta difícil su comprobación.

9. Por su naturaleza pueden ser: dolosos, intencionales, culposos o imprudenciales.

10. Los menores de edad tienen facilidad de cometerlos.

11. Tienden a extenderse, por lo que requiere una urgente regulación jurídica" (Téllez Valdés, 2004, p. 163).

Existen otros puntos que hay que tomar en consideración:

- No es la computadora la que atenta contra el hombre, es el hombre el que encontró una nueva herramienta, quizás la mas poderosa hasta el momento, para delinquir.

- No es la computadora la que afecta nuestra vida privada, sino el aprovechamiento que hacen ciertos individuos de los datos que en ellas contienen.

- La humanidad no está frente al peligro de la informática sino a individuos sin escrúpulos con aspiraciones de obtener el poder que significa el conocimiento.

- Por eso la amenaza futura será directamente proporcional a los adelantos de las tecnologías informáticas.

- La protección de los sistemas informáticos puede abordarse desde distintas perspectivas civil, comercial, administrativa. (Recuperado 3 de junio de 2007 de http://www.segu-info.com.ar/delitos/informacionydelito.htm)

2.2.4. Clasificación de los delitos informáticos

Para poder clasificar a los delitos informáticos, “habría que preguntarse primero que clase de actividades, contenidos y derechos relacionados con los sistemas informáticos y/o Internet pueden regularse, y que actos en especifico pueden constituir un delito o ilícito” (Molina Salgado, 2003, p. 164).

La tecnología informática en cuanto a su contenido, actividades y derechos, podemos decir que se puede regular.

Es así como podemos ver que todos los derechos tanto de usuarios como de proveedores pueden ser regulados más de proveedores, ya que son ellos los que tienen la responsabilidad de que la información que por su servicio pasa no sea usada para fines delictivos, lo mismo sucede con otras instituciones, incluyendo las de gobierno.

Es por esto que recae una gran responsabilidad a todas las instituciones públicas o privadas que tengan algo que ver con el manejo de datos, ya que de ellas depende que no se den actos que constituyan un delito informático que atente o afecte el bien jurídicamente tutelado.

No obstante, “al no existir por el momento más que un delito de tipo informático, en la legislación penal federal, seria complicado hacer una clasificación legal objetiva que sirva para conocer los diferentes tipos y los alcances y efectos de las actividades ilícitas que se realizan en los medios informáticos” (Molina Salgado, 2003, p. 21).

Es difícil dentro de nuestra legislación hacer de igual forma una clasificación de ilícitos informáticos ya que la referencia y regulación de este tema es muy escaso y en algunos casos, no existe.

Julio Téllez Valdés da una clasificación dependiendo de la conducta delictiva que utiliza a la computadora como instrumento para la comisión de un ilícito:

Computadoras como medio

- Falsificación de documentos vía computarizada (tarjetas de crédito, cheques etcétera.)
- Variación de los activos y pasivos de la situación contable de una empresa.
- Planeación o simulación de delitos convencionales (robo, homicidio, fraude etcétera.)
- Robo de tiempo de computadora.
- Lectura sustracción o copiado de información confidencial.
- Modificación de datos tanto a la entrada como a la salida.

- Aprovechamiento indebido o violación de un código para penetrar a un sistema introduciendo instrucciones inapropiadas (esto es lo que se conoce en el medio como el método del Caballo de Trolla).

- Variación en cuanto al destino de pequeñas cantidades de dinero, hacia una cuenta bancaria apócrifa, método conocido como la “técnica del salami”.

- Uso no autorizado de programas de cómputo.

- Introducción de instrucciones que provocan “interrupciones” en la lógica interna de los programas, a fin de obtener beneficios.

- Alteración en el funcionamiento de los sistemas.

- Obtención de información residual impresa en papel o cinta magnética luego de la ejecución de trabajos.

- Acceso a áreas informatizadas en formato no autorizado.

- Intervención en la línea de comunicación de datos o teleproceso (Téllez Valdés, 2004, p. 165).

Existe otra categoría que encuadra a las conductas criminológicas que van dirigidas a la computadora, accesorios o programas como entidad física, a ésta se le llama como fin u objetivo.

- Programación de instrucciones que producen un bloqueo total al sistema.

- Destrucción de programas por cualquier método.

- Daños a la memoria.

- Atentado físico contra la máquina o sus accesorios (discos, cintas, terminales etcétera.)

- Sabotaje político o terrorismo en el que se destruya o surja un apoderamiento de los centros neurológicos computarizados.

- Secuestro de soportes magnéticos en los que figura la información valiosa con fines de chantaje, pago de rescate etcétera (Téllez Valdés, 2004, p. 166).

Esta clasificación es lo más cercano que se tiene a los delitos que se cometen, pero es de vital importancia que se realice una clasificación más precisa y actual ya que teniendo una clasificación que abarque y explique con detalle cuales son los delitos e ilícitos, dará la pauta para que se reduzca el número de conductas delictivas que tengan que ver en el ámbito de la informática.

2.2.5. Categorización de los delitos informáticos

Los términos tales como “delincuencia cibernética”, “delito informático” y “delito en redes de computadoras” carecen de definiciones aceptadas universalmente.

En el Congreso Sobre Redacción de Legislación en Materia de Delitos Cibernéticos de la OEA (2004 27 de enero), se muestra que parte de la confusión que surge de su uso se debe a que en la actualidad los delincuentes utilizan las computadoras en el curso de la comisión de todo tipo de actos ilícitos. El papel que desempeña la computadora en el marco de la comisión de un delito puede sin embargo entrar en alguna de las tres categorías que se indican a continuación:

A) La computadora como herramienta.

La computadora puede utilizarse como herramienta para la comisión de actividades delictivas. En esta categoría de uso se incluyen delitos que generalmente se cometían en el mundo físico, pero que en la actualidad ocurren cada vez con más frecuencia en el marco de la Internet.

Entre los mencionados actos ilícitos encontramos las actividades fraudulentas, la distribución de pornografía infantil, las violaciones de derechos de propiedad intelectual, las amenazas y persecuciones, el lavado de dinero y la venta en línea de sustancias y artículos ilegales. Sin embargo los dispositivos de comunicación en línea pueden utilizarse también para concretar una amplia gama de actos ilícitos comunes. Por ejemplo, las sesiones de chateo o de correo electrónico pueden utilizarse para planear o coordinar todo tipo de delitos, e incluso para transmitir amenazas o comunicaciones de extorsión a las víctimas.

En su mayor parte, las leyes del “mundo físico” ya norman estos tipos de conductas ilegales.

Es importante que los legisladores examinen las leyes penales tradicionales a fin de asegurarse de que los actos no permitidos en el mundo físico queden también prohibidos en el virtual.

Los delincuentes pueden utilizar las redes de computadoras en varias formas a efecto de cometer actos ilícitos tradicionalmente concretados en el mundo físico, por ejemplo, ciertas comunicaciones en Internet son del tipo “punto a punto”, como las llamadas telefónicas, en tanto que otras transmiten información a un público vasto y desconocido, como sucede en el caso de los periódicos.

Las prohibiciones legislativas deben ser neutrales desde el punto de vista tecnológico, de forma tal que las normas legales no queden desactualizadas frente a los desarrollos técnicos.

B) La computadora como instrumento de almacenamiento de información.

Al igual que las empresas, los gobiernos y los ciudadanos; los delincuentes aprovechan la capacidad que poseen las computadoras para almacenar gran cantidad de información. Estos últimos almacenan datos durante la comisión de los diferentes tipos de delitos tradicionales, y dicha información se convierte en un elemento probatorio en soporte electrónico que se pone de relieve al momento de realizar la investigación del acto ilícito. Por ejemplo, un narcotraficante puede usar su computadora portátil o su Palm Pilot para almacenar una lista de clientes. De igual forma, un secuestrador podría redactar en su computadora el pedido de rescate de la víctima, lo cual serviría como un vínculo que los investigadores podrían usar para llegar hasta él. Además, la información guardada en una computadora puede servir para resolver un acto ilícito aún en el caso de que el delincuente no lo haya creado.

A modo de ejemplo pongamos el caso de una investigación en situación de defraudación, en la que se presentaron facturas falsas por bienes o servicios, la resolución de la misma puede depender de la información de la base de datos de la empresa defraudada, en la que figuran los pagos y cuentas.

En el Congreso Sobre Redacción de Legislación en Materia de Delitos Cibernéticos de la OEA (2004 27 de enero) se plantea que si bien el uso de computadoras como instrumentos de almacenamiento de datos no exige la sanción de nuevas leyes sustantivas, el aumento de volumen de pruebas electrónicas puede ser suficiente para que un país considere la modificación de las normas que rigen el acceso de las fuerzas del orden a dichos elementos probatorios.

C) La computadora como blanco del delito.

Las computadoras pueden también ser objeto de actos ilícitos, los cuales se denominan generalmente “delitos cometidos contra una red informática” y consisten de

ataques a la confidencialidad, integridad o disponibilidad de los sistemas informáticos o computacionales.

Los delincuentes ejecutan este tipo de actos a fin de obtener datos almacenados en el sistema atacado. También lo hacen para controlar el sistema en forma gratuita o sin contar con autorización o bien para eliminar o modificar datos o interferir la información de la computadora o el funcionamiento de la misma. Muchas veces estos ataques se traducen en robos de información o en pérdidas pecuniarias para el propietario de la computadora afectada.

Las actividades delictivas que se incluyen en esta categoría son las intrusiones a computadoras, envío de virus y demás códigos perjudiciales, “desconfiguración” de sitios Web y ataques del tipo “denegatoria de servicio”, que afectan el funcionamiento de los datos o de los sistemas computacionales.

Este análisis examina los marcos jurídicos necesarios para tratar las situaciones descritas, en las que la computadora resulte como blanco de las actividades delictivas.

2.3. Regulación penal los delitos informáticos

La sociedad ha demostrado tener una gran dependencia a los medios informáticos, por eso es que el derecho penal empeñado en combatir una nueva clase de delincuencia, necesita un estudio más a fondo a fin de evitar que las nuevas conductas no tipificadas sigan generando daños irreparables a los integrantes de esta nueva sociedad de la información.

“El Derecho Penal requiere que los legisladores estatales y federales, realicen modificaciones a los Códigos Penales, y se adapten a los nuevos tiempos, así como a revisar la legislación ya existente para su adaptación, también hace falta que la ciencias criminologicas se adapten y tengan las herramientas necesarias para apoyar a

la materia del Derecho, asimismo, es necesario contar con personal adecuado capaz de realizar investigaciones relacionadas con este tipo de delitos, por ejemplo, peritos en la materia e investigadores, también es importante que este delito sea perseguido por el estado, ya que éste es el único con la capacidad suficiente para realizar esta tarea, ya es hora de que se incluyan este tipo de delitos especiales para la nueva sociedad de la información" (Téllez Valdés, 2004, p. 165).

Es por esto que el Derecho Positivo en esta materia ayudaría mucho a su desarrollo, para que sea lo suficientemente completa, para que así todas las formas que busquen los delincuentes informáticos puedan ser objeto de investigación, mediante técnicas y métodos nuevos que deben ser implementados por el Derecho.

2.4. Medidas de seguridad para evitar los delitos informáticos

Todos los días "se roban autos todos los días, por lo que es probable que tome algunas medidas como poner los seguros, estacionarse en un estacionamiento o utilizar una alarma" (Norton, 2006, p. 537).

De igual forma se "debe estar consiente de las amenazas que enfrentan sus computadoras y datos y tomar medidas para protegerlos" (Norton, 2006, p. 537).

Las redes de Internet han creado posibilidades infinitas para que las personas trabajen, se comuniquen, aprendan, compren, vendan, jueguen e interactúen con otras personas de todas partes del mundo, todas estas posibilidades provienen de la apertura de las redes o Internet, el cual está disponible prácticamente a todas las personas y para todos los tipos de uso, sin embargo, la gran apertura que hace que Internet sea tan valioso también hace que sea una puerta a muchas amenazas.

No es posible culpar al Internet de los delitos informáticos, ya que éste es solo y únicamente atribuible al hombre, ya que es éste quien hace mal uso de la tecnología

para cometer ilícitos relacionados con este medio, por ejemplo, el robo de identidad, piratería, virus, etcétera.

Unas de esas medidas de seguridad con el fin de cuidar y protegernos a nosotros mismos es “la conciencia. Debe entender todos los peligros que amenazan específicamente a un sistema de cómputo. Debe conocer la forma en que cada amenaza puede afectarle y considerarla de acuerdo con esto” (Norton, 2006, p. 537).

Otra medida de seguridad sería respaldar todos los datos que contenga nuestra computadora, esta es una solución en contra de la amenaza de la pérdida de datos.

Existen dos clases de recomendaciones para protegernos:

- La primera: proteger y respaldar información del usuario en contra de daños personales, por ejemplo pérdida de información personal, registros financieros y médicos.

- La segunda: asegurar al sistema de cómputo, en contra de daños físicos, como es el robo, vandalismo, problemas de energía y desastres naturales o ataques a los datos que están almacenados en la computadora.

Los ladrones informáticos hacen uso de tecnología simple y también de la alta tecnología, con el fin de obtener la información que necesitan, por ejemplo, debemos cuidar lo siguiente:

- El navegar por encima de sus hombros, es simplemente que una persona observe como introduce información de identificación personal, para realizar transacciones, por ejemplo, en cajeros automáticos.

- La interferencia, es decir, la obtención de información personal de manera indebida a través de la intromisión de llamadas telefónicas u otra forma.

- Otra técnica muy sencilla para estos delincuentes es la de robar correo de los buzones que tienen información personal, así como el apoderarse de la basura, en la que pueden encontrar mucha información a través de los estados de cuenta o información de cuentas de cheques, con estos datos ellos ganan obteniendo números de cuentas que pueden utilizar.

- Como hemos podido ver en últimas fechas el delincuente puede valerse de métodos muy sofisticados o muy simples, por ejemplo, el de engañar a su víctima con el fin de que proporcione información importante bajo el pretexto de que es alguien de un banco o que proporciona algún servicio y solo quiere verificar algunos datos, ganando la confianza de la víctima, solicitándole números confidenciales, contraseñas, para así poder acceder a su cuenta directamente desde el sitio de la red del banco.

- Como hemos podido ver existen muchas facetas y formas en las que un delincuente puede obtener información, por ejemplo, solo necesita una computadora y una conexión de Internet, para poder interceptar información mediante programas como los caballos de Troya, que colocados en un sistema interceptan toda la información necesaria, este tipo de delitos no es tan común ya que requiere el uso de alta tecnología.

- El revisar los reportes de crédito de todos los movimientos que se realizaron y si se encuentra cualquier error reportarlo inmediatamente.

- Es bueno conservar todos los documentos, reportes bancarios y estados de cuenta por lo menos durante tres años, esto ayudaría a evitar problemas y aclarar cualquier error o anomalía que pueda surgir.

- Verificar cuando se quiera comprar algo en línea, que el sitio es seguro antes de proporcionar información (Norton, 2006, p. 539).

Es por esto que con respecto a los ordenamientos jurídicos nacionales, la respuesta dada frente a la delincuencia informática es inexistente o resulta insuficiente, más si se atiende al carácter transfronterizo que conlleva a la utilización de una red como Internet. (Recuperado 3 de junio de 2007 de http://www.davara.com/preguntas/delitos.html#3)

El ordenamiento jurídico que regula esta situación es el derecho penal, es por eso la inquietud de complementar esta regulación con otras medidas complementarias o alternativas que sirvan para dar respuesta a esta cuestión.

2.4.1. Amenazas y grado de daños

“El concepto general de la seguridad de cómputo es eliminar las amenazas o protegerse en contra de ellas. Una amenaza es cualquier cosa que puede ocasionar daños. En el contexto de la seguridad de computo, una amenaza puede ser un ladrón, un virus, un terremoto o un simple error del usuario” (Norton, 2006, p. 538).

Las “amenazas por si mismas no causan ningún daño a menos que explote una vulnerabilidad existente” (Norton, 2006, p. 538).

Es decir que si existe alguna debilidad que no se haya protegido en contra de amenazas, ésta abre instantáneamente la posibilidad de un daño, por ejemplo, un automóvil sin seguro es vulnerable a un robo, esta vulnerabilidad no tiene ningún significado a menos que un ladrón de autos se encuentre cerca del vehículo, pero es probable que al saber esto los vehículos sean estacionados bien cerrados y en lugares seguros para evitar el robo del vehículo, lo mismo pasa con las computadoras sabemos

que hay delincuentes informáticos por lo que debemos tener precauciones en nuestros equipos de cómputo.

Es muy probable que los equipos de cómputo sean infectados por virus si es que no se utilizan antivirus y más si la computadora se mantiene conectada a la red, es por esto que se puede determinar el grado de daños que distintas amenazas pueden ocasionar a un equipo y saber que posibilidades de amenazas pueden llegar.

Cuando se protege un sistema de cómputo es recomendable pensar en los posibles daños que nos podrían afectar, ya sea un virus; piratas los cuales nos pueden hacer perder una gran cantidad de datos, sin contar los desastres naturales, los cuales ocasionarían los mismos problemas de pérdida e información.

“El propósito de una computadora es procesar datos de alguna manera para crear información. El objeto de la seguridad de cómputo es proteger este proceso” (Norton, 2006, p. 548).

Debido a lo anterior, es que la información y los datos son intangibles, la finalidad de este propósito es difícil, no obstante se debe intentar proteger todo lo que tenga valor de cualquier amenaza latente; existen tres categorías de amenazas, los cuales son: Malware, Virus y Programas Maliciosos.

Comencemos diciendo que “el término Malware, describe virus, gusanos, programas de ataque como el de Caballo de Troya, estos representan la amenaza más común a la información” (Norton, 2006, p. 548).

Los virus como ya lo habíamos visto son programas que se pegan a programas anfitriones; los gusanos atacan las redes extendiéndose a otras máquinas de cualquier red a la que estén conectadas realizando ataques previamente programados; los Caballos de Troya introducen códigos maliciosos en el interior de un programa útil.

El crimen cibernético

Va encaminado “a robar la computadora, dañar la información o robarla” (Norton, 2006, p. 548).

El uso de una computadora para llevar a cabo un acto criminal es una amenaza que crece cada día, los delitos más frecuentes que se realizan en este rubro son: fraude, establecimiento de sitios Web bancarios fraudulentos, los cuales utilizan para robar información de cuentas de clientes, fraude en subastas, falta de entrega de productos, fraudes con tarjetas de crédito.

La piratería informática.

Esta “sigue siendo la forma más común de crimen cibernético y continua creciendo en popularidad” (Norton, 2006, p. 549).

El pirata informático es aquella persona que utiliza una computadora y red, para introducirse dentro de otra computadora, para cometer un acto ilegal, esto puede ser el principio de un ataque mayor, esta actividad permite que el pirata informático controle la computadora o computadoras, para realizar ataques por diversión, ataques a empresas, ataque a sistemas de inteligencia, ataques terroristas, etcétera.

Este tipo de ataques representa una invasión a la privacidad y representan un gran daño a la economía y se cree que este tipo de ataques podría ser la herramienta de las guerras futuras.

2.4.2. Medidas para contrarrestar daños

Para evitar amenazas y con el fin de proteger la información de los sistemas de cómputo, siempre es conveniente tener un respaldo de toda la información, contra la amenaza de pérdida de datos.

Otra medida es el de tener mucho cuidado, ya que es muy probable que se comparta con otras personas muchos tipos de información y sobretodo personal, no sabemos en manos de quien cae toda esa información, por eso es conveniente que no proporcione datos de cuentas a través del teléfono, ya que recordemos ellos tienen esos datos, tampoco es conveniente el manejar números de cuenta, contraseñas por correo electrónico, ya que como hemos podido ver no es una forma segura de transmitir información, ya que puede ser interceptada, también al comprar en línea es conveniente saber que tan seguro es el sitio en el que pensamos hacer una compra antes de introducir información.

“Por todos estos inconvenientes necesitamos tener precaución para protegernos en contra de robo del identidad, uno de esos es mantener lejos a las personas que intentan vender un producto por Internet, ya que solicitan información para saber lo más posible, realizando campañas de marketing” (Norton, 2006, p. 539).

“Es recomendable tener dos direcciones de correo una solo para las personas de confianza y otra para todo lo demás, ya que esta recibirá todo lo no deseado y dejará libre la otra, no corriendo el riesgo de perder información” (Norton, 2006, p. 540).

CAPITULO III

MARCO JURÍDICO DE LA DELINCUENCIA INFORMÁTICA EN MÉXICO

3.1. Análisis del derecho a la información y la libertad de expresión dentro de la constitución

Dentro de la historia de la humanidad se han dado acontecimientos fundamentales que la han transformado y que han permitido trascender y plasmar sus pensamientos, uno de ellos es la invención del alfabeto, por los fenicios, lo que permitió plasmar los pensamientos, posteriormente el invento de la imprenta por Gutemberg, esto permitió difundir a mayor número de personas el pensamiento, otro es la invención de la energía eléctrica, la cual es la que se vive en este momento y permitió la creación de medios electrónicos, mismos que dejan que la comunicación sea más rápida, en tiempo real y visualizando a la otra persona.

"En todo estado de derecho las instituciones e individuos que lo integran se encuentran regidos por normas jurídicas, mismas que establecen una serie de derechos y obligaciones, las cuales tienen el objeto de establecer un desarrollo permanente dentro de la sociedad" (Orozco Gómez, 2001, p 3).

Es por eso que todos y cada uno de los miembros de una sociedad al llevar acabo su rol deberán de observar las disposiciones que rijan su actividad, esto lo podemos relacionar con los medios de comunicación y el derecho, al regular su función.

Recordemos que dentro de nuestra constitución se encuentra regulada la libertad de expresión, en el sentido y función de los medios de comunicación electrónicos, así como también dentro de la Ley Federal de Imprenta, Ley de Radio Televisión y Cinematografía, así como en la Ley Federal de Derechos de Autor.

Estos marcos jurídicos definen los límites de libertad de expresión y el derecho a la información.

Por otro lado, el Código Penal Federal y los Códigos Penales estatales limitan la libertad de expresión mediante el concepto de difamación.

“El artículo 6º constitucional define la libertad de expresión y al derecho a la información en general. El artículo 7º amplia estos derechos y los conceptualiza en términos de su ejecución, específicamente en cuanto al oficio de escribir y del periodismo” (Barrios Garrido 1998, p. 33).

En cuanto a la manifestación de ideas podemos decir que Internet, es un espacio que se caracteriza en este sentido y en “consecuencia se encuentra sujeto a las limitaciones impuestas al ejercicio de la libertad de expresión por el artículo 6º, es decir las ideas expuestas en Internet son permisibles siempre y cuando no ataquen a la moral, los derechos de terceros ni provoquen algún delito o perturben el orden público” (Barrios Garrido 1998, p. 33).

El artículo 6º constitucional, como ya se había mencionado párrafos anteriores, consagra lo que conocemos como libertad de expresión, esto es que garantiza a todo individuo que se encuentra dentro de nuestro país, la libertad de expresar libremente sus ideas.

“Este artículo contiene dos tipos de garantías, una de carácter individual (derecho público subjetivo) que es la libertad de expresión y otra de tipo social (porque abarca a toda la sociedad) que es el derecho a la información” (Orozco Gómez 2001, p. 8).

La libertad de expresión se refiere “exclusivamente a la manifestación de las ideas producidas de manera individual por medio de la palabra, los gestos o cualquier otra forma susceptible de ser captada de manera auditiva o visual, quedando protegida la

expresión artística en el marco del contenido del precepto constitucional" (Orozco Gómez 2001, p. 8).

La libertad de información en Internet es un fenómeno interesante e importante, ya que esta gran red permite la difusión y el acceso a gran número de información, sin olvidar los derechos de propiedad intelectual y tanto internacionales como locales.

Hasta la fecha Internet no se ha tipificado en ninguna ley, pero si se señala como medio de comunicación masiva, enfrentándonos a un problema interpretativo ya que al no existir una interpretación de los términos que se expresan con claridad seguiremos con limitaciones en el ejercicio de la libertad de expresión, ahora también cualquier intento de definición sería dar pie a grandes debates en esta materia.

Es por esta razón que gran parte de la información que podemos encontrar en Internet, nos puede traer grandes problemas en cuanto a la moral, ya que para algunos algo que es inmoral para otro no lo es, es por eso que se necesita una regulación en cuanto a los contenidos de Internet y de la liberta de expresión.

"Los puntos de partida para evaluar las implicaciones de Internet en el derecho a la información y la libertad de expresión en México son:

a) Las actuales normas relacionadas a este tema.

b) La relación dinámica y contradictoria entre el avance tecnológico y estas normas, aplicadas en el contexto socioeconómico y político en México.

c) El impacto en el derecho comparado de las corrientes de pensamiento y acontecimientos actuales en torno a la red que se han generado fuera de nuestro país" (Barrios Garrido 1998, p. 31).

La libertad de expresión del pensamiento se encuentra reconocida dentro de nuestra constitución, esta manifestación de ideas en esta época moderna es muy amplia, ya que se cuenta con múltiples medios de comunicación, en los que puede transmitir sus ideas o sus sentimientos.

Es por esto que podemos decir que “el artículo 6º constitucional es igualmente el fundamento de la libertad de la comunicación, ya que los medios para manifestar las ideas son indispensables a las personas como vías necesarias para tales manifestaciones” (V. Castro, 1998, p 114).

Ya que el artículo 6º, señala límites a la forma de manifestar las ideas, lo que no señala o precisa son los instrumentos que se pueden utilizar para manifestar las ideas, dejando abierto a los diversos medios de comunicación la manifestación de éstas.

Es por esto que decimos que nuestra constitución no precisa ni tiene en cuenta todas las problemáticas que pueden darse ya que ésta fue hecha en un tiempo en el que no se concebían los avances informáticos de hoy en día.

Para entender un poco más transcribimos dichas disposiciones:

> Artículo 6º La manifestación de ideas no será objeto de ninguna inquisición judicial o administrativa, sino en el caso de que ataque a la moral, los derechos de tercero, provoque algún delito, o perturbe el orden público; el derecho a la información será garantizado por el Estado.
>
> Artículo 7º Es inviolable la libertad de escribir y publicar escritos sobre cualquier materia. Ninguna ley ni autoridad puede establecer la previa censura, ni exigir fianza a los autores o impresores, ni coartar la libertad de imprenta, que no tiene más límites que el respeto a la vida privada, a la moral y a la paz

> pública. En ningún caso podrá secuestrarse la imprenta como instrumento del delito.
>
> Las leyes orgánicas dictarán cuantas disposiciones sean necesarias para evitar que, so pretexto de las denuncias por delito de prensa, sean encarcelados los expendedores, “papeleros”, operarios y demás empleados del establecimiento donde haya salido el escrito denunciado, a menos que demuestre previamente la responsabilidad de aquéllos.

Es muy claro que dentro de las disposiciones transcritas no debe existir ninguna limitación a la libertad de expresión del pensamiento, por tanto, “debería establecerse con toda claridad en el texto constitucional, y no a base de interpretación” (V. Castro, 1998, p. 120).

En otra disposición penal es bien sabido que “se ordena que salvo la naturaleza de las cosas y las posibilidades materiales, se secuestren o incauten los instrumentos que fueron utilizados para cometer un delito” (V. Castro, 1998, p. 120).

En el caso de delito de imprenta, y con rango constitucional esto se prohíbe, dando a entender que en ningún caso será secuestrada la imprenta como instrumento del delito, entonces cuando hablemos de computadoras que se utilizan para la comisión de un delito que ataque la moral, afecte derechos a terceros o a la vida privada, que perturbe la paz y el orden público, éstas ¿podrán o no ser incautadas?

Estos son dilemas a los que nos enfrentamos debido a que se debe establecer una legislación clara y no basarse de las interpretaciones para evitar problemas de esta índole ya que se dejan desprotegidos a los agentes encargados de realizar una investigación.

Debido a estos problemas es de llamar la atención que todavía no se regulen muchas materias como por ejemplo la de delitos informáticos.

3.2. Regulación de Internet

En nuestro país la posibilidad de que se regule Internet no se ha realizado; su uso gira alrededor de códigos éticos y la tendencia es que será un fenómeno autorregulable.

A pesar de la difusión del Internet, muchos legisladores no entienden el concepto y la estructura de Internet, lo mismo pasa con los jueces y magistrados del Poder Judicial.

“El hecho es que se tiene que regular Internet; nuestro país ha dado lugar a múltiples controversias entre usuarios, la mayoría de ellos académicos y políticos. Por un lado se encuentran aquellos que insisten en que deben reglamentarse la información dentro de Internet, como cualquier otro medio, ya sea radio, televisión o prensa; por el otro están aquellos que piensan que la censura electrónica viola la libertad de expresión y que después con el argumento de contenidos prohibidos se podrá bloquear el acceso a la información”. (Barrios Garrido 1998, p. 20).

Este es un “problema serio ya que para compaginar las leyes locales con el mundo de las redes y de acuerdo con que criterio se establecerán las reglas del juego” (Barrios Garrido 1998, p. 21).

La Ley Federal de Telecomunicaciones omite el concepto de Internet, mismo que se interpreta como un concepto de valor agregado.

Es decir que lo define como el servicio que presta un usuario de la red concesionada o red pública de telecomunicaciones, cuya actividad tiene efecto en el

formato, contenido, código, protocolo, almacenaje o aspectos de la información transmitida.

Un prestador de servicios de valor agregado sólo necesita registrarse ante la Secretaria de Comunicaciones y Transportes.

“Como parte del mundo de las telecomunicaciones, podemos deducir que Internet puede vincularse como campos diversos de la legislación federal referentes a inversión extranjera, competencia económica, propiedad intelectual e industrial, asuntos de carácter fiscal, de procedimiento administrativo, comunicación social, tratados comerciales, seguridad pública, entre otros” (Barrios Garrido 1998, p. 22).

La política en materia de informática dictada por el poder ejecutivo federal, va dirigida a la promoción y al fomento de una nueva cultura de la educación a través de los medios informáticos.

La verdad es que dentro de nuestras leyes existen lagunas que impiden resolver problemas innumerables en especial:

“a) Régimen aplicable a los servicios ofrecidos a través de Internet.

b) Régimen de la publicidad, de todo tipo.

c) Régimen de la venta a distancia.

d) Régimen aplicable a la formación de contratos y transacciones electrónicas y el comercio cibernético.

e) Régimen del trabajo a distancia o teletrabajo.

f) Cuestiones de seguridad en redes y protección de datos.

g) Violación al derecho a la privacidad.

h) Responsabilidad por difusión de información o de imágenes difamatorias que causen daño moral o que atenten contra el orden público.

i) Control y sanción de criminalidad específica que den lugar a nuevos delitos" (Barrios Garrido, 1998, p. 24).

Es indudable que Internet se utiliza hoy en día en todas las actividades que realizamos, lo cual implica múltiples relaciones jurídicas que, si bien están contempladas como instituciones dentro de los códigos y leyes, pocas de ellas resuelven la complejidad del empleo de nuevas tecnologías.

Es entonces que nos encontramos con un nuevo reto no solo legislativo sino de carácter social, que permita que Internet, sea utilizado en todas las ramas de la sociedad.

3.3. Violación a la intimidad

La intimidad y la privacidad, "básicamente se refieren a los ámbitos en los cuales los terceros no tienen un estricto derecho del conocimiento de la información del sujeto pasivo" (Campoli, 2005, p. 65).

Es por eso que las nuevas técnicas de procesamiento de la información, sumadas a los métodos de transmisión de las mismas, plantean problemas que hasta la fecha no han sido previstos por las leyes.

“Algunos de los tipos penales existentes resultan claramente aplicables a las nuevas modalidades aunque estas se realicen por medios informáticos” (Campoli, 2005, p. 65).

Es por esto que resulta violentada la privacidad o la intimidad, un ejemplo de esto es la violación de secretos, no importando si se divulgan en forma oral, escrita o electrónica, pero existen otros que surgen directamente de la aplicación de las nuevas tecnologías.

Las intrusiones mediante las cuales se accede a información confidencial pueden llegar a afectar seriamente la privacidad de los datos.

En el Congreso Sobre Redacción de Legislación en Materia de Delitos Cibernéticos de la OEA (2004, 27 de enero), se estableció que el perjuicio no resulta fácil de cuantificar en términos monetarios, por ejemplo, un caso que tuvo lugar en EU, en el que un grupo de piratas informáticos ingresó ilegalmente a la base de datos de un prestador de servicios de salud, robando información médica personal de una persona famosa.

Este acto, en sí mismo, no causó un gran perjuicio económico, aunque fue una significativa violación de la privacidad.

El legislador que redacte la norma que penalizará estos actos deberá prever las sanciones adecuadas que tengan un efecto disuasivo respecto de los mismos.

Además, el legislador podrá tomar en cuenta la sensibilidad especial que revisten ciertos tipos de información, previendo así penas más severas para los delincuentes que se apoderen ilegalmente de esos datos, por ejemplo, el robo de determinados registros del gobierno o de cierta información sobre seguridad nacional supone un daño de tal magnitud que exige una pena más grave, independientemente del valor pecuniario que tengan dichos datos.

De igual modo, el legislador puede determinar que su país enfrenta un problema delictivo específico, optando entonces por imponer penas más estrictas a los casos de robo de información que contribuyan a estimular dicho problema. Muchos países, por ejemplo, se enfrentan a lo que se conoce como “robo de identidad”, ilícito que consiste en apropiación no autorizada de la identidad de un tercero a fin de obtener créditos en forma fraudulenta o de retirar fondos de su cuenta bancaria.

En estas circunstancias, el legislador podrá imponer penas especiales a las intrusiones que involucren el robo de datos financieros o personales, tales como registros bancarios, números de tarjetas de crédito, informes crediticios e información personal.

3.3.1. Información privada

La información privada la podemos definir como “aquella en la que el titular posee un derecho exclusivo de uso o de conocimiento pero que en mayor o menor medida es conocida por un grupo de personas a su alrededor y por el estado, respondiendo a fines de garantía de los derechos del ciudadano” (Campoli, 2005, p. 64).

Esto es por ejemplo “cuando utiliza una tarjeta para rentar películas o hacer compras, sus hábitos de consumo son rastreados electrónicamente en una variedad de sistemas comerciales, estos son registrados en una base de datos, al igual que registros médicos, financieros y de crédito están a disponibles para cualquier persona que esté autorizada para verlos” (Norton, 2006, p. 540).

La información privada como se dice en la definición, existe además del titular otras personas que con derecho conocen la información del titular.

Es por eso que muchas de las tiendas y compañías con las que tratamos diariamente mantienen bases de datos con información de todos nosotros, y es

sorprendente saber que aparte de tener en sus bases de datos nuestros nombres y direcciones, también pueden saber, cuantas veces vamos al súper y que es lo que compramos.

El problema es que muchas de estas “compañías no mantienen esta información de manera confidencial; es posible que la vendan a otras compañías que están interesadas en saber de usted” (Norton, 2006, p. 540).

La información personal es un producto comercial que muchas empresas aprovechan para venderla, a esto se le llama extracción de datos.

“La extracción de datos es un proceso para obtener inteligencia empresarial que todas las organizaciones grandes, desde bancos hasta tiendas de comestibles, emplean con el fin de analizar datos computarizados” (Norton, 2006, p. 540).

Estas compañías utilizan patrones de conducta de los individuos que utilizan para un tratamiento especial, este método de extraer información obtiene muchos millones de dólares al año y crece rápidamente y no existen leyes que lo regulen, esta información en otras manos podría ocasionar muchos dolores de cabeza.

Podemos entonces tomar como parámetro para constituir como delito la divulgación no autorizada a terceros, la lesión al bien jurídico, esto “se constituirá en delito, para el sujeto activo que no tenga derecho expreso” (Campoli, 2005, p. 64).

Es evidente el hecho de que “el conocimiento de información de un tercero resulta imposible de probar, lo que debe penarse es cualquier acción que implique que el sujeto activo esté en posesión de información del sujeto pasivo a la cual no tenia derecho” (Campoli, 2005, p. 65).

3.3.2. Información íntima

Como una aproximación a este tema, podemos decir que la información íntima, “es aquella sobre la cual el titular tiene la absoluta exclusividad de su conocimiento y divulgación, que se encuentra ligada a su proceso interno de selección y no puede ser conocida ni aun en circunstancias especiales por persona alguna ni por el estado” (Campoli, 2005, p. 65).

Se representa como la esfera de la intimidad, se encuentra ligada expresamente según su raíz etimológica a lo que tiene que ver con el fuero interno de la persona, lo cual lo separa de la información privada.

Es decir, dentro de esto se encuentran los valores internos, la orientación sexual y decisiones morales, es por eso que la información íntima “debe ser protegida desde todas las esferas posibles ya que la integran los que se llaman en doctrina datos sensibles y cualquier conocimiento o divulgación no autorizada produce necesariamente un daño” (Campoli, 2005, p. 65).

Este problema, de que ojos extraños husmean en los archivos y directorios, se ha dado desde el nacimiento de la tecnología de la información, por los llamados hackers, cuya intención principal es investigar lo que contiene una computadora y los crackers, quienes se dedican a romper barreras de protección de las computadoras, para robar información.

“Se abre un campo muy amplio para los abogados, que tendremos que aprender mucho acerca de la tecnología informática para poder legislar y hacer valer las leyes y el derecho a la intimidad que se viola constantemente al compartir información mediante Internet” (Ferreira Cortes, 2006, p. 43).

3.3.3. ¿Qué son las nettiquett?

La rapidez con que actúa la tecnología en estos días hace que la sociedad intensifique los intercambios culturales, los cuales se desarrollan al mismo tiempo que surgen modelos jurídicos, no escritos, creándose en los últimos tiempos una cultura universal de Internet.

Sobre lo que está permitido y no dentro de Internet, se deben hablar en sus propias políticas y normas, “aunque existen, también, reglas no escritas, que constituyen la conocida como nettiquette” (Barrios Garrido 1998, p. 12).

“La netiquette, (etiqueta de la red, ciberetiqueta, ciberurbanidad) Conjunto de normas dictadas por la costumbre, experiencia y sentido común que define las reglas de urbanidad y buena conducta que deberían seguir los usuarios de Internet en sus relaciones con otros usuarios. (Téllez Valdés, 2006, p. 484).

Cuando nos comunicamos con otras personas frente a frente o por teléfono, utilizamos gestos, expresiones y/o modulaciones de la voz que ayudan a nuestro interlocutor a interpretar nuestro mensaje. Estas importantes ayudas audio visuales de la comunicación no están presentes en la comunicación escrita por lo que es más difícil transmitir ciertas ideas, conceptos o sentimientos. (Recuperado 12 de junio de 2007 de http://www2.netexplora.com/biblioteca/netiquettes.html)

Las netiquettes son “una serie de reglas de etiqueta que todos debemos conocer y seguir al comunicarnos a través de la red para una comunicación más efectiva y un mejor uso de los recursos y el tiempo. Debido a las características particulares del medio es necesario utilizar algunos convencionalismos que ya se han establecido para comunicarnos efectivamente y evitar los malos entendidos, ofender o ser ofendidos, así como un sin número de otras cosas negativas que pueden surgir al no conocerlos. (Recuperado 12 de junio 2007 de http://www2.netexplora.com/biblioteca/netiquettes.html)

Además del sentido común, los buenos modales, la cortesía, el respeto, la consideración y la tolerancia, éstas son algunas reglas que debemos observar al comunicarnos a través de la red:

- Tenga siempre en mente que al otro lado de la pantalla hay un ser humano real, con sus propias ideas y sentimientos, siempre escriba como si lo estuviera mirando a los ojos, nunca escriba algo que no le diría frente a frente a otra persona, esta es una regla que debe tener siempre presente.

- Mensajes enviados a listas de distribución de correo-e serán recibidos por todos los miembros. Mantenga en sus mensajes personales a otros miembros en privado y envíe a la lista solo aquellos mensajes que desee compartir y sea de interés para todos.

- Mantenga sus comunicados breves y al grano.

- No envíe a la lista anexos largos como archivos gráficos. De hacerlo así se corre el riesgo de que no lleguen a su destino.

- Al contestar algún mensaje indique de que se trata para que se sepa a que se está refiriendo.

- Nunca conteste un e-mail cuando esté enojado o molesto.

- Respete las leyes sobre derechos reservados.

- Sea cuidadoso con la información personal o privada. No publique datos de terceros, por ejemplo dirección o números de teléfono.

- Nunca cite en público correos-e que le fueron enviados en privado.

- Cerciorese de que está enviando un correo-e al destinatario correcto.

- Las letras mayúsculas se pueden utilizar para sustituir acentos o enfatizar, pero no escriba todo en mayúsculas pues esto se interpreta como que usted está gritando.

- No utilice para promocionar causas religiosas, filosóficas, políticas, comerciales o para promover su propio sitio Web.

- Sea tolerante, recuerde que el botón de borrar permite ignorar cualquier mensaje indeseado.

- De sentirse ofendido por algo o alguien dirija sus quejas en privado al ofensor, al igual críticas y desacuerdos. Las felicitaciones en público.

- Si recibe un mensaje de aviso sobre un virus, no escriba a los demás para alertarlos, lo más seguro es de que se trate de falsas alarmas que abundan en la red.

- No es aceptable el uso de vocabulario obsceno, sin embargo, se permiten siempre y cuando se especifique que es un chiste, debiendo hacer la aclaración antes de que lo lean.

- Cuando se ingresa a una nueva cultura es susceptible cometer errores sociales. Quizás se pueda ofender a personas sin querer hacerlo o tal vez lo que otros dicen se puede mal interpretar. (Recuperado 12 de Junio de 2007 http://www2.netexplora.com/biblioteca/netiquettes.html)

- Intente siempre estar relajado y permanecer tranquilo en una discusión. A menudo uno lee mal los significados de otras personas en un mensaje y lo toma como una crítica o un sarcasmo.

- Intente poner en su mensaje un título que indique la importancia o no de su mensaje con el fin de que la gente lo vea.

- No envíe los correos en mayúsculas, ya que esto demuestra que usted esta gritando o irritado quizás, utilice en sus mensajes la mezcla de mayúsculas y minúsculas

- Si usted está preguntando es necesario hacer la pregunta porque, así es más fácil conseguir una respuesta, si usted fija una pregunta es más fácil recibir una respuesta.

- La mayoría de la gente que no está familiarizada con el mundo de la computadora, tiene la impresión de que los lugares de charla son para personas que no tienen nada que hacer, y no necesariamente, es por eso que se tiene que respetar la identidad y la credibilidad de la persona en la red.

- Identificar correctamente con un título de un mensaje, especialmente si es un correo oficial, esto ayuda a darnos cuenta del contenido del mensaje. (Recuperado 12 de Junio de 2007 http://pakavenue.com/webdigest/it_corner/intro_006.htm)

- Ser discreto al usar emoticons, ya que el uso excesivo distrae. (Recuperado 12 de Junio de 2007 de http://pakavenue.com/webdigest/it_corner/intro_006.htm)

Por lo tanto, cuando alguien cometa un error sea comprensivo, quizás si el error es mínimo no sea necesario comentarlo, siempre piense antes de reaccionar, tener

buenos modales no nos da derecho a corregir a los demás, si es necesario informar a alguien de algún error, debemos hacerlo siempre cortésmente, y en privado, por sobre todas las cosas no ser arrogante con los demás. (Recuperado 12 de Junio de 2007 http://www2.netexplora.com/biblioteca/netiquettes.html)

3.4. Breve referencia del delito informático en México

El Internet puede utilizarse como un medio para cometer toda una serie de delitos que están tipificados en el Código Penal mexicano y en la mayoría de leyes criminales alrededor del mundo.

"La información que viaja por Internet puede ser empleada por crakers, hackers o piratas, o puede emplearse como medio para la transmisión de pornografía descrita en el artículo 200 del Código Penal; incluso Internet puede ocuparse como medio de transmisión de información entre bandas de narcotraficantes" (Barrios Garrido, 1998, p. 99).

Como instrumento de la comisión de un delito, podría decomisarse una computadora o una pequeña red, sin embargo, resultaría imposible hacerlo con un elemento intangible como Internet.

El artículo 40 del Código Penal Federal, establece que los instrumentos del delito, así como las cosas que sean objeto o producto de él, se decomisarán si son de uso prohibido.

Si son de uso lícito, se decomisarán cuando el delito sea intencional.

Las autoridades competentes procederán al inmediato aseguramiento de los bienes que podrán ser materia de decomiso, durante la averiguación o en el proceso.

El artículo 16 de la Constitución es otro ordenamiento que podría “aplicarse al correo electrónico, pues establece: La correspondencia que bajo cubierta circule por las estafetas, estará libre de todo registro y su violación será penada por la ley” (Barrios Garrido 1998, p. 100).

Es decir que el artículo 16 de la Constitución representa el marco jurídico de la privacidad en nuestro país, ya que consagra una de las garantías más importante que es el derecho a no ser molestados en nuestra persona, familia, domicilio, papeles o posesiones, sino solo a través de mandamiento por escrito de la autoridad competente que funde y motive la causa legal del procedimiento.

Es importante señalar que en materia penal la ley no puede aplicarse por analogía; respecto al delito de violación de correspondencia, podría aplicarse lo dispuesto en el artículo 173 del Código Penal Federal, el cual señala que:

- “Se aplicará de 3 a 180 jornadas de trabajo a favor de la comunidad.

- Al que abra indebidamente una comunicación escrita que no este dirigida a él.

- Al que indebidamente intercepte una comunicación escrita que no esté dirigida a él, aunque la conserve cerrada y no se imponga de su contenido”.

Los delitos previstos en este artículo se persiguen por querella.

Los delitos informáticos constituyen una gran laguna en nuestras leyes penales, es por eso que se requiere un análisis urgente por parte de legisladores, penalistas y académicos.

“Hoy en día es posible codificar la información a través de programas especiales, tarjetas electrónicas con claves de acceso o sistemas que después de cada operación

generan una nueva clave para que pueda leer la información el destinatario final" (Barrios Garrido, 1998, p. 103).

Lo anterior permite realizar transacciones o envío de información con mayor seguridad, pero recordemos que el avance de la tecnología es muy rápido, y las prácticas delictivas más comunes, por lo que es imperativo que se legisle respecto a este importante tema.

3.4.1. Legislación sobre delitos informáticos

Un análisis de las legislaciones que se han promulgado en otros países, arroja que las normas jurídicas que se han puesto en vigor están dirigidas a proteger la utilización abusiva de la información reunida y procesada mediante el uso de computadoras, e incluso en algunas de ellas se ha previsto formar órganos especializados que protejan los derechos de los ciudadanos amenazados por los ordenadores. (Recuperado 11 de Junio de 2007 de http://www.monografias.com)

En la actualidad en nuestro país nos falta mucho por hacer a nivel de legislación, no existen figuras jurídicas adecuadas en ley alguna, no son perseguibles como delitos.

La falta de una adecuada tipicidad nos obliga a usar analogías que, como señalamos con anterioridad, no se aplica en materia penal, "por lo que se entiende que tales conductas hasta ahora, y solo que ingresen a otros tipos de delitos como el fraude, violación a derechos de autor o propiedad intelectual, o daños que puedan ser probados, serían perseguibles solo civilmente" (Barrios Garrido, 1998, p. 104).

Es por eso que en últimas fechas hablar de leyes que regulen Internet se ha convertido en una moda entre los legisladores, pero por lo visto no es algo que les importe mucho.

“El tema pareciera novedoso, pero en realidad es que lleva ya algún tiempo sobre la mesa. En Mayo de 2000 entraron en vigor una serie de reformas al hoy Código Civil Federal, Código de Comercio, Código Federal de Procedimientos Civiles y Ley Federal de Protección al Consumidor. Su finalidad era la de contratación electrónica por medios electrónicos, ópticos o cualquier otra tecnología que pudiera considerarse válidos obligatorios y exigibles entre las partes que concurran a su celebración”. (Recuperado 12 de julio de 2007 http://www.isocmex.org.mx/kiyoshi.html)

El texto de esta ley fue un acierto de los legisladores de nuestro país, ya que sentó una base para los negocios electrónicos mexicanos en el área global, lo que es una realidad es de que ninguno de estos documentos han entrado en vigor por lo que el comercio en electrónico no ha despegado en nuestro país con la intensidad esperada. (Recuperado 12 de julio de 2007 http://www.isocmex.org.mx/kiyoshi.html)

La verdad es que “los empresarios, directivos, y demás personas con poder de decisión dentro de las corporaciones mexicanas no saben qué esperar, pues enfrentan riesgos considerables y difíciles de determinar en la mayoría de los casos; a su vez, sus consejeros y abogados no saben con precisión cuál será la reacción de las autoridades judiciales y administrativa al aplicar la ley en operaciones mensajes de datos y/o medios de autenticación electrónicos. Después de todo, la autoridad tampoco cuenta con los medios indispensables para llevar acabo tal interpretación. Y es precisamente en este escenario donde aparece la iniciativa de “Ley Federal de Firma y Comercio Electrónicos, Mensajes de Datos y Servicios de la Sociedad de Información” (Recuperado 12 de Junio de 2007 http://www.isocmex.org.mx/kiyoshi.html).

Dicha reforma se trata de un proyecto ambicioso mismo que se encuentra motivado en beneficio del país.

“Dicha reforma promovida por el diputado Barbosa “aglomera demasiados y muy diversos tipos de regulación, pertenecientes a ramas muy distintas del derecho, en una

sola iniciativa de ley en la que saltan a la vista temas tan diversos como la prestación de servicios de la sociedad de la información, regulación de contenidos (relacionado con temas de nuestra garantía constitucional de libertad de expresión), otros como los excluyentes de responsabilidad para los proveedores de servicio de Internet, colocándolo como un simple sujeto pasivo en la transmisión de información, almacenamiento de información, alojamiento de páginas Web". (Recuperado 12 de Julio de 2007 de, http://www.isocmex.org.mx/kiyoshi.html)

Dichas reformas tocan también asuntos como el valor probatorio de los mensajes electrónicos, mismo que ya ha sido regulado en el Código Federal de Procedimientos Civiles, así como la privacidad de la información, comunicaciones publicitarias no solicitadas, firma electrónica y medios de certificación de las mismas, contratación electrónica y formación del consentimiento por medios electrónicos (Recuperado 12 de Junio de 2007 de, http://www.isocmex.org.mx/kiyoshi.html).

Esta reforma resulta ser algo complicada, y muestra lo difícil que resulta aplicarla a nuestras autoridades y lo inseguro que resulta ser para todos la aplicación de ésta.

En otros países en los que ya se cuenta con leyes relacionadas con el entorno digital, la técnica legislativa es ordenada, ya que contienen una serie de leyes separadas entre si, regulando de forma concisa, sólida y delimitada cada materia bien delimitada, y tomaron en cuenta a miembros de la sociedad consultando con ellos e identificando las necesidades y solucionando los problemas que pudieran surgir, siempre velando por el bien común. (Recuperado 12 de Junio de 2007 de http://www.isocmex.org.mx/kiyoshi.html)

Debido a las complicaciones que se tienen en la regulación de esta materia existen algunas personas que opinan que "a menor regulación las cosas funcionan mejor, esto es con menos trabas burocráticas, sin embargo, si debe de regularse pues caemos en

la anarquía informática y la fuente de los problemas en Internet es a causa de la falta de regulación de este medio a nivel local y mundial.

“Uno de los desafíos que tiene nuestro país es aumentar el nivel de protección de las computadoras en los hogares, por que en ocasiones el usuario ni siquiera se ha dado cuenta de que su equipo está infectado. (Recuperado 12 de Junio de 2007 de http://espanol.news.yahoo.com/s/06062007/4/negocios-falta-regulaci-n-internet-fuente-delitos-l-nea-experto.html)

3.4.2. Estados de la república que ya cuentan con un tipo penal informático dentro de su legislación

Los delincuentes en México así como la tecnología, avanzan a pasos agigantados y adquieren conocimientos cada vez mayores en el ámbito informático y de la ley, ya que como sabemos no son cualquier tipo de personas, conocen perfectamente los alcances que esta puede tener; se apoyan de la tecnología para cometer sus delitos, es por eso que los legisladores y toda la sociedad, tenemos una ardua tarea de creación de leyes o modificar las ya existentes para lograr una eficaz protección de los bienes jurídicos de interés social.

Los estados de la república que no cuentan con alguna mención de conductas que pudieran estar relacionadas con el uso de instrumentos informáticos, como medio de comisión del delito o de las cuales los mismos resulten objeto material del delito son las siguientes:

- Código Penal para el Estado de Baja California Sur;
- Código Penal para el Estado de Campeche;
- Código Penal para el Estado libre y soberano de Chiapas;

- Código Penal para el Estado libre y soberano de Chihuahua;
- Código Penal de Coahuila;
- Código Penal para el Estado libre y soberano de Durango;
- Código Penal para el Estado de Hidalgo;
- Código Penal para el Estado de Michoacán;
- Código Penal para el Estado libre y soberano de Oaxaca;
- Código Penal para el Estado de Querétaro;
- Código Penal para el Estado de San Luis Potosí;
- Código Penal para el Estado libre y soberano de Tlaxcala;
- Código Penal para el Estado libre y soberano de Veracruz;
- Código Penal para el Estado de Sonora. (Campoli, 2005, p. 74).

Es importante señalar que es preocupante que estos estados hasta la fecha no contengan dentro de sus legislaciones el delito informático; se requiere de una actualización para evitar que este delito sobrepase su legislación y cuando se cometa el delito no se castigue por no haberse considerado, ya que la tecnología no solo se encuentra en algunos lugares, sino en todas partes, y el fin del estado es proteger a los ciudadanos.

Estados de la república que si contienen tipificado los delitos informáticos o electrónicos son:

- Código Penal para el Estado de Aguascalientes.

En su Libro Primero, Título Tercero, que habla de “Circunstancias Modificadoras de la Punición”, delitos de querella, y establece lo siguiente:

Artículo 23.- Acceso sin autorización y al daño informático como delitos graves y delitos de acción privada, etcétera.

El Libro Segundo, de las figuras típicas, título Vigésimo Primero, que habla de “Delitos Contra la Seguridad de los medios Informáticos y Magnéticos”, establece:

Artículo 223.- Acceso sin autorización consistente en interceptar, interferir, recibir, usar o ingresar por cualquier medio sin autorización debida, etcétera.

Capítulo II. Daño informático.

Artículo 224.- El daño informático consiste en la indebida destrucción o deterioro parcial o total de programas, archivos, bases de datos o cualquier otro elemento como sistemas o redes de computadoras, etcétera.

Artículo 225.- El acceso sin autorización o el daño informático se cometa culposamente, etcétera.

Artículo 226.- La falsificación informática consiste en la indebida modificación, alteración o imitación de los originales de cualquier dato, archivo o elemento contenido en sistema de redes, etcétera.

- Código Penal para el Estado de Baja California.

En el Libro Segundo, en la Parte Especial, Título Tercero, de “Delitos Contra la Inviolabilidad del Secreto”, señala:

Capítulo Único. Revelación de Secretos.

Artículo 175, Habla solamente al que sin consentimiento divulgue un secreto por medios electrónicos y se persigue por querella, etcétera.

- Nuevo Código Penal para el Estado de Colima.

Este menciona en su Libro Primero, Título Segundo de “Delito y Delincuente” y establece:

Artículo 10.- Hace referencia al artículo 157 bis del mismo código y lo considera como grave, etcétera.

El Libro Segundo, en su Título Quinto, de “Delitos Contra la Moral Pública” indica:

En su Capítulo II, que habla sobre “Corrupción de Menores”, establece:

Artículo 157 bis.- Habla sobre realizar actos de exhibicionismo corporal por medios electrónicos, etcétera.

En su Sección Quinta, de “Delitos Contra el Medio Ambiente”, de su Título Único, del Capítulo Único, de “Delitos Ambientales”.

Artículo 224.- Habla sobre la alteración de programas de computo para realizar verificación de vehículos, etcétera.

- Código Penal para el Estado de México

En su Libro Segundo, de “Delitos Contra el Estado”, subtítulo Cuarto, de “Delitos Contra la Fe Pública”, Capítulo IV, de “Falsificación y Utilización Indebida de Títulos al Portador, Documentos de Crédito Público y Documentos Relativos al Crédito” señala:

En su artículo 174 menciona:

Fracción IV. Habla sobre el delito de alteración de medios de identificación electrónica de tarjetas, títulos o documentos, etcétera.

Fracción V. Habla sobre acceder indebidamente a los equipos electromagnéticos, de tarjetas o títulos o documentos para el pago de bienes y servicios, etcétera.

- Código Penal para el Estado de Guanajuato.

En su Libro Segundo, Parte Especial, Título Tercero de los “Delitos Contra las Vías de Comunicación de Uso Público y Violación de Correspondencia”, Capítulo Segundo, Violación de Correspondencia.

El artículo 231 menciona:

Fracción I.- Habla sobre la intercepción o retención de comunicación, etcétera.

Fracción II.- Habla sobre la destrucción alteración de comunicación o información contenida en equipos de cómputo, etcétera.

- Código Penal para el Estado de Guerrero.

Señala en su Libro Segundo, Parte Especial, Título X, de “Delitos Contra de las Personas en su Patrimonio”, del Capítulo I, Robo.

En su artículo 165

Fracción I.- Al que se apodere de una cosa propia, que se halla por cualquier título en poder de otro y, etcétera.

Fracción II.- Aprovechamiento de programas computarizados, señales televisivas o de Internet, sin consentimiento, etcétera.

- Código Penal para el Estado Libre y Soberano del Estado de Jalisco.

En el Libro Segundo, de Delitos en Particular, Título Décimo Cuarto, de los “Delitos Contra la Paz, Libertad y Seguridad de las Personas”, Capítulo VII, Secuestro.

Artículo 194

Fracción I, inciso k), habla de que para lograr el secuestro, se valga de redes de computadoras o de otros medios de alta tecnología, para lograr su fin, etcétera.

- Código Penal para el Estado de Morelos

En su Libro Segundo, Parte Especial, de “Delitos Contra el Individuo”, Título Décimo Segundo, de “Delitos Contra la Moral Pública”, Capítulo I, “Ultraje a la Moral Pública” establece:

Artículo 213

Fracción I.- Al que ilegalmente fabrique reproduzca, imágenes obscenas y que las exponga o que haga circular, etcétera.

Fracción II.- Al que realice exhibiciones públicas obscenas por cualquier medio electrónico, incluyendo Internet, etcétera.

Capítulo III.- Corrupción de menores e incapaces, etcétera.

Artículo 213 quater.

Habla sobre el facilitar o introducir por cualquier medio a los menores o a un incapaz para realizar actos de exhibicionismo corporal, lascivos o sexuales, con el fin de videograbarlo, fotografiarlo, o exhibirlo en medios electrónicos, incluyendo Internet, etcétera.

- Código Penal para el Estado de Nuevo León.

En el Libro Segundo, de su Título Décimo Noveno, de “Delitos en Relación con el Patrimonio”, del Capítulo I, Robo, indica:

Artículo 365

Fracción IV, habla sobre el apoderamiento material de los documentos que contengan datos de computadoras, aprovechamiento o utilización de los mismos, sin derecho y sin consentimiento, etcétera.

- Código de Defensa Social para el Estado Libre y Soberano de Puebla.

En su Capítulo Décimo, “Falsedad”, Sección Primera, de “Falsificación de Acciones, Obligaciones y otros Documentos de Crédito Público” establece:

Artículo 245 bis

Fracción IV.- Al que altere, copie o falsifique medios de identificación electrónica, cintas o dispositivos magnéticos de tarjetas, títulos, etcétera.

Fracción V.- Al que acceda indebidamente a los equipos o sistemas de cómputo o electromagnéticos de las instituciones emisoras de tarjetas de crédito.

Artículo 246

En caso de que el infractor sea funcionario o empleado público, etcétera.

Artículo 247.

Si el infractor fuera abogado, se le inhabilitará para el ejercicio de su profesión, etcétera.

En su Libro Segundo, Capítulo Séptimo, sección segunda, de “Corrupción de Menores e Incapaces”.

Artículo 224 ter

El que por cualquier medio, sea directo, mecánico o con soporte informático, o de cualquier otro tipo, venda publique, distribuya o exhiba y difunda, material informático infantil, etcétera.

- Código Penal para el Estado Libre y Soberano de Quintana Roo

En su Capítulo II, de “Falsificación de Documentos y Uso de Documentos Falsos” establece:

Artículo 189 bis

Fracción III.- Habla del que copie o reproduzca, altere los medios de identificación electrónicas cintas o dispositivos magnéticos para el pago de bienes o servicios, etcétera.

Fracción IV.- Al que accese indebidamente a equipos y sistemas de cómputo o electromagnéticos de las instituciones emisoras de tarjetas, etcétera.

- Código Penal para el Estado de Sinaloa

En su Título Décimo, de Delitos Contra el Patrimonio, de su Capítulo V, “Delito Informático”, señala:

Artículo 217.- Comete delito informático, la persona que dolosamente y sin derecho:

Fracción I.- Use o entre a una base de datos, sistema de computadores o red de computadoras o cualquier parte de la misma, con el propósito de alterar un esquema o artificio, con el fin de defraudar, obtener dinero, bienes o información o

Fracción II.- Intercepte, interfiera, reciba, use, altere, dañe o destruya un soporte lógico programa de datos de una base, sistema o red.

- Código Penal para el Estado de Tabasco.

En su Titulo Décimo Primero, de “Delitos Contra la Seguridad de la Comunicación”, del Capítulo V, “Violación de la Comunicación Privada” señala.

Artículo 316

Habla sobre quien intervenga la comunicación privada de terceras personas a través de medios eléctricos o electrónicos, etcétera.

- Código Penal para el Estado de Tamaulipas.

En su Título Quinto, de “Delitos Contra la Moral Pública”, Capítulo II, referente a “Corrupción de Menores Incapaces, Pornografía Infantil y Prostitución Sexual de Menores Incapaces” establece:

Artículo 194 bis.

Fracción I. Habla sobre el que obligue a menores a cometer actos de exhibicionismo corporal, lascivos, sexuales o pornográficos, con el fin de videograbarlos, fotografiarlos y exhibirlos mediante medios electrónicos.

En el Título Séptimo, de Delitos de Revelación de Secretos y de Acceso Ilícito a Sistemas y Equipos de Informática, del Capítulo II, Acceso Ilícito a Sistemas y Equipos de Informática establece:

Artículo 207 bis

Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática, protegidos por un sistema de seguridad, etcétera.

Artículo 207 Ter.

Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de cómputo de alguna dependencia pública protegida por algún sistema, etcétera.

Artículo 207 cuater.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática de alguna dependencia pública protegida por algún mecanismo, etcétera.

Artículo 207 quinquies.

Al que está autorizado para acceder a sistemas y equipos informática de alguna dependencia pública, indebidamente modifique, destruya o provoque pérdida de información, etcétera.

Artículo 207 sexies.

Al que estando autorizado para acceder a sistemas y equipos de informática de alguna dependencia pública, indebidamente copie, transmita o imprima información, etcétera.

En su Título décimo noveno, de “Delitos en Relación con el Patrimonio de las Personas”.

Artículo 400.

Fracción IV. El apoderamiento material de los documentos que contengan datos de computadoras o el aprovechamiento o utilización de dichos datos, sin consentimiento, etcétera.

- Código Penal para el Estado de Yucatán.

En su Capítulo II, referente a “Corrupción de Menores e Incapaces, Trata de Menores y Pornografía Infantil” indica:

En su artículo 211 menciona.

Al que facilite por cualquier medio a menores de dieciséis años con o sin su consentimiento, a realizar actos de exhibicionismo corporal, con objeto de videograbarlos, fotografiarlos o exhibirlos por medios electrónicos, con fin de lucro, etcétera.

- Código Penal para el Estado de Zacatecas.

En su Libro segundo, de “Delitos en Particular”, Título Sexto, de “Delitos Contra la Moral Pública”.

Capítulo II Corrupción de menores.

Artículo 183 Bis.

Comete el delito de corrupción de menores.

En su Fracción II, Quien proporcione o permita que menores, presencien, por medio de aparatos electrónicos, la exhibición de audio visual, etcétera.

- Nuevo Código Penal para el Distrito Federal.

En su Libro Segundo, Parte Especial, Título Vigésimo Cuarto, de “Delitos Contra la Fe Pública”, en su Capítulo I, referente a, Producción, Impresión, Enajenación, Distribución, Alteración, o Falsificación de Títulos al Portador y Documentos de Crédito Público o Vales de Canje, establece:

Artículo 336.

Fracción IV. Altere los medios de identificación electrónica de tarjetas, títulos o documentos para el pago de bienes y servicio;

Fracción V. Acceda a los equipos electromagnéticos de las instituciones emisoras de tarjetas, títulos o documentos para el pago de bienes o servicios o para disposición de efectivo;

Fracción VI. Adquiera, utilice o posea equipos electromagnéticos o electrónicos para sustraer la información contenida en la cinta o banda magnética de tarjetas, títulos o documentos, para el pago de bienes o servicios o para disposición de efectivo, etcétera.

Fracción VII. A quien utilice indebidamente información confidencial o reservada de la institución o persona que legalmente este facultada para emitir tarjetas, títulos o documentos utilizados para el pago de bienes y servicios, o de los titulares de dichos instrumentos o documentos.

En el Título vigésimo quinto, que habla sobre “Delitos Contra el Ambiente y la Gestión Ambiental”, en su Capítulo II, de “Delitos contra la Gestión Ambiental”.

Artículo 347 bis.

Fracción I. Altere, permita la alteración u opere en forma indebida cualquier equipo o programa utilizado para la verificación vehicular prevista en las disposiciones jurídicas aplicables en el Distrito Federal;

En su Título décimo quinto, de “Delitos Contra el Patrimonio”, en su Capítulo III, Fraude

Artículo 231.

Fracción XIV. Para obtener algún beneficio para si o para un tercero, por cualquier medio accese, entre o se introduzca a los sistemas o programas de informática del sistema financiero o indebidamente realice operaciones, transferencias o movimientos de dinero o valores, independientemente de que los recursos no salgan de la institución.

3.4.3. ¿Cómo se establece el delito informático en el Código Penal Federal?

En el Código Penal Federal se establece una gama de figuras delictivas, en su Libro Segundo, Título Noveno, referente a “Revelación de Secretos y Acceso Ilícito a Sistemas y Equipos de Informática” en su Capítulo II “Acceso Ilícito a Sistemas y Equipos de Informática” indica:

Artículo 211 bis 1.

El que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, etcétera.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, etcétera.

Artículo 211 bis 2.

Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, etcétera.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, etcétera.

Artículo 211 bis 3.

Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente modifique, destruya o provoque pérdida de información, etcétera.

Al que estando autorizado para acceder a sistemas y equipos de informática del estado, indebidamente copie información, etcétera.

Artículo 211 bis 4.

Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, etcétera.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, etcétera.

Artículo 211 bis 5.

Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente modifique, destruya o provoque pérdida de información, etcétera.

Título vigésimo sexto, de los “Delitos en materia de Derechos de Autor”.

Artículo 424 bis.

Fracción I. A quien produzca, reproduzca, introduzca al país, almacene, transporte, distribuya, venda o arriende copias de obras, fonogramas, videogramas o libros protegidos por la Ley Federal del Derecho de Autor, en forma dolosa, con fin de especulación comercial y sin autorización, etcétera.

A quien a sabiendas, aporte o provea de cualquier forma, materias primas o insumos destinados a la producción reproducción de obras, fonogramas, videogramas o libros, etcétera.

Fracción II. A quien fabrique con fin de lucro un dispositivo o sistema, cuya finalidad sea desactivar los dispositivos electrónicos de protección de un programa de computación.

CAPITULO IV

ANÁLISIS JURÍDICO PARA PREVENIR Y COMBATIR LA DELINCUENCIA INFORMÁTICA

4.1. La norma constitucional mexicana ante los avances informáticos

La problemática a la que nos enfrentamos es complicada debido a las conductas desarrolladas por los criminales cibernéticos, es por esto que resulta indispensable crear las herramientas necesarias y suficientes en el derecho, para evitar acciones que puedan vulnerar a bienes jurídicos que se intentan proteger por considerarlos importantes para el desarrollo de la sociedad.

La utilización de Internet originó una normatividad no escrita, cuyos usuarios se basaban en usos sin reglas formales basadas en consideraciones de tipo ético.

Nuestra constitución se ha ido adecuando a la dinámica de nuestra sociedad para cumplir con sus requerimientos, ya que ésta constituye la mejor garantía de la vigencia del estado de derecho, pero en lo que respecta a este tema, falta mucho para alcanzar el nivel de importancia que debe de tener, ya que las estructuras importantes que son las constitucionales siguen siendo las mismas desde mucho tiempo atrás, dejando un andamiaje jurídico inestable.

De nuestro actual texto constitucional es necesario observar que existen disposiciones que necesitan ser adecuadas a la realidad de las necesidades, otras que deberían quedar fuera de la misma, porque corresponden a disposiciones generales que para el momento y tiempo en que vivimos ya son obsoletas.

Recordemos que nuestra constitución que actualmente nos rige data del año de 1917, obviamente sufriendo modificaciones durante el transcurso de los años, cambiando según las necesidades y adecuándose a los cambios de la sociedad.

Es por esto que se necesita ampliar más nuestra normatividad ya que hasta la fecha Internet, se ha convertido en una herramienta importante, siendo un soporte a infraestructuras de importancia crítica en el campo de la energía, el transporte, áreas bancarias y financieras, generando también un papel importante en las actividades de las empresas y en los mecanismos de prestación de servicios que el estado proporciona a los ciudadanos y a la comunidad empresarial, además de servir como medio de intercambio de información y comunicación.

Debido a lo anterior es necesario que este tema tome importancia, ya que hasta la fecha no la ha tenido para los legisladores, dejando la incógnita ¿cuando nos enfrentemos a un problema y al no existir una interpretación que se exprese con claridad, tendremos que hacerlo por analogía? esto en el derecho penal no es aceptado, por ende, nos enfrentamos a un problema con grandes limitaciones.

Es de destacarse el papel del Estado, el cual aparece como el principal e indelegable regulador de la actividad de control de flujo de información a través de redes informáticas.

Dentro de nuestra constitución se encuentra regulada la libertad de expresión y el derecho a la información, del primero podemos decir que Internet es un espacio que se caracteriza por la libertad de expresar todo tipo de ideas de manera individual auditiva y visual, lo cual no es así, ya que a pesar de que en su artículo 6º indica que la expresión de las ideas expuestas en Internet son permisibles, nos marca limites los cuales no deben atacar a la moral, derechos de terceros ni provoquen algún delito o perturben el orden público.

Es decir que “en el ejercicio de las garantías no puede atacar a la moral; a los derechos de terceros o a la vida privada; provocar algún delito; o perturbar la paz o el orden público, exponiendo nuestra opinión de que todas esas áreas de no afectación o perturbación mediante el ejercicio de estas garantías, deben estar en leyes respectivas

específicas y en los términos precisos de éstas, sin posibilidades de interpretaciones subjetivas de los funcionarios que deben aplicarlas al caso concreto” (V. Castro, 1998, 119).

De esta forma podemos decir que es importante la creación o modificación de leyes que reglamenten el ejercicio de dichas garantías constitucionales.

4.2 Problemática de la legislación penal en las entidades federativas

Como hemos podido observar en el capítulo anterior, existen estados de la república que hasta la fecha no cuentan con legislación legal alguna referente a conductas que pudieran estar relacionadas con el uso de instrumentos informáticos como medios de comisión de delitos, por otra parte de los estados que ya cuentan con legislación, el “40% de las ya existentes el mejor comentario posible es que se requiere de inmediata actualización a fin de evitar que los cambios tecnológicos y conductas de los posibles sujetos activos que ya están vulnerando bienes jurídicos en algunos casos protegidos y en otros cuya necesidad de protección es inmediata” (Campoli, 2005, p. 75).

Es importante ver que se necesita una legislación urgente debido al gran avance tecnológico, así como la actualización de las mismas, ya que como podemos ver en legislaciones de diferentes estados existen incongruencias como por ejemplo, en el Código Penal para el Estado de Aguascalientes, que considera “a las conductas descritas como delitos graves y por la otra, las instaure como delitos de acción privada que se persiguen por querella” (Campoli, 2005, p. 77).

Dentro de la materia penal podemos observar que es contradictorio, ya que las conductas delictivas graves deben perseguirse de oficio ya que están afectando el bien jurídico que el Estado tiene la obligación de proteger.

Otro punto importante es el definir los términos con que se clasificará esta materia ya que como se comentó anteriormente, entre el hombre y la máquina existe una forma de comunicación, y para esto se necesita especificar los términos y el lenguaje a utilizar con que se podrá definir cada conducta o instrumento que se utilice para cometer el delito, esto nos permite especificar bien los delitos para no dejar desprotegidos ni excluir ningún objeto, conducta o instrumento.

Esto evitará que no existan lagunas legales, para así obtener una legislación más completa que contenga todo lo necesario para evitar que los delincuentes encuentren dentro de la ley paraísos de impunidad.

De esta manera se darán los lineamientos necesarios, ya que lo que se ha podido observar entre legislaciones de los estados, es que algunos de estos solo copian el mismo texto que en otro ya se legisló, conteniendo los mismos errores, que son copiados de donde fue sacada, estos errores son arrastrados por todas las demás legislaciones que los copian, es por esto que es fundamental que se haga un estudio por parte de los legisladores a fondo y que se verifiquen las necesidades y problemáticas a las que se enfrenta cada entidad federativa, ya que no son las mismas vicisitudes en los diversos estados de la república.

Lo mismo pasa con legislaciones de otros países, que son copiadas para reglamentar un problema que tal vez no se encuentre o no se de con la misma regularidad como de donde fue copiada.

4.3. Análisis de elementos para una reforma en materia de delitos informáticos

Los bienes jurídicos que se encuentran a merced de los cibercriminales deben ser protegidos por el estado, esta tarea no es fácil y por eso resulta indispensable crear herramientas para evitar estas conductas ya que recordemos que los infractores al tener conocimiento del alcance que tiene la ley es muy fácil evadirla; recordemos que

estamos hablando de personas que tienen conocimientos y habilidades en el uso de sistemas y no presentan el denominador común de un delincuente.

Estas normas deberán ser analizadas para su comprensión y “evitar la creación de normas que pudieran resultar perfectas en la teoría pero inútiles en la práctica” (Campoli, 2005, p. 152).

Es claro que nos enfrentamos a un problema y que tal vez a los ojos de algunas personas resulta difícil de resolver, pero se debe poner atención y capacitar a las autoridades, y verificar todos los escenarios posibles como la extraterritorialidad de los delitos, la probabilidad de identificar a los sujetos activos al cometer sus actividades delictivas en la red, el encuadramiento del delito, etcétera.

4.3.1. Protección del bien jurídico en el derecho penal

Bien es todo aquello que representa un valor para las personas, es por eso que nuestras legislaciones deben “proteger los valores elementales de conciencia, de carácter ético social, que constituyen el fundamento más sólido que sustenta al Estado y a la sociedad” (Osorio y Nieto, 2005, p. 10).

Independientemente de la teoría o la opinión personal de cada persona se puede decir que “el bien jurídico representa los valores, los intereses de las personas físicas o morales protegidas por las normas mediante la sanción correspondiente” (Osorio y Nieto, 2005, p. 10).

Los bienes jurídicos pueden proteger intereses o valores individuales, sociales, del Estado o en el caso de los sistemas federales, de las entidades federativas y de personas morales, es por eso que se les clasifica como “personales, cuando tutelan los intereses de los personas físicas y/o de las personas morales, y suprapersonales, si protegen los intereses de la sociedad y del Estado” (Osorio y Nieto, 2005, p. 11).

La protección de los bienes jurídicos, se lleva acabo por medio de las normas penales; “en el sistema jurídico mexicano, estas normas se encuentran contenidas en el Código Penal Federal, en el nuevo código penal del Distrito Federal, en los códigos penales de cada entidad federativa y en diversas leyes federales que tipifican conductas delictivas” (Osorio y Nieto, 2005, p. 11).

Los códigos penales cuentan con una parte en la que contienen diversas figuras típicas que ayudan de mejor manera la protección de los bienes jurídicos.

“En cuanto a la clasificación de los delitos, existen diversos criterios o sistemas; por lo que se refiere al orden en que aparecen, en algunos códigos se presentan al principio de los delitos que afectan los bienes jurídicos de las personas físicas, otros códigos inician el libro correspondiente con los delitos que atacan bienes jurídicos de la sociedad o del estado; algunos ordenamientos agrupan los delitos con base en la objetividad jurídica tutelada, o bien jurídico protegido; otros clasifican los delitos en razón del sujeto activo o del pasivo, y también encontramos como criterio rector en este orden de ideas, el agrupar los delitos atendiendo la materia que regulan, así como por el delito en si” (Osorio y Nieto, 2005, p. 12).

El bien jurídico no es una mera elaboración teórica, al contrario tiene su base dentro de la Constitución, es por eso que se ordena categóricamente en sus artículos lo siguiente:

Artículo 14.- Nadie podrá ser privado de la vida, de la libertad o de sus propiedades, posesiones o derechos…

Artículo 16.- Nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones…

Como podemos observar la constitución siendo la norma de mayor jerarquía, “protege determinados valores o intereses que considera fundamentales para el ser humano, los eleva a rango de garantías individuales y mediante ordenamientos secundarios, el Código Penal, protege en concreto tales bienes” (Osorio y Nieto, 2005, p. 13).

El objeto del bien jurídico, es el de ayudar a precisar el objeto de protección, facilitando el conocimiento y comprensión de delitos.

4.3.2. Principios del bien jurídico

En la sociedad actual siempre ha existido la necesidad de aplicar penas corporales, debido a que la humanidad no ha podido vivir sin sanciones que regulan la vida social y jurídica para lograr la estabilización y la paz sociales.

“Hasta hoy no se vislumbra una alternativa distinta del penoso hecho de tener que marginar al hombre de la vida en sociedad cuando no respeta el orden jurídico.” (Salas Campos, 2001, p. 95).

Es por esta razón que el derecho penal se concibe “como un instrumento creado y pactado por el hombre en sociedad que responde categóricamente contra las conductas que ponen en peligro el orden y la tranquilidad sociales” (Salas Campos, 2001, p. 95).

Por otra parte “la pena es utilizada como un instrumento que coadyuva a restablecer la paz social y es un recurso no querido ni deseado, pero necesario e inevitable” (Salas Campos, 2001, p. 95).

La pena es el último recurso que es utilizado para resolver situaciones que ponen en peligro la tranquilidad social, pero un medio imprescindible.

El derecho penal es el encargado de proteger bienes jurídicos cuando el comportamiento antisocial los lesiona, para esto cuenta con principios fundamentales los cuales ayudan a preservar los bienes jurídicos penales y son, fragmentarios, subsidiarios y de última ratio.

4.3.3. Carácter fragmentario, de última ratio y subsidiario del derecho penal

Como ya se comento, el derecho penal es el encargado de salvaguardar los bienes jurídicos contra determinadas agresiones específicas, su función se lleva a cabo mediante amenazas, como factor disuasivo y de aplicación de penas.

“En un sistema penal dentro de un Estado democrático de derecho, el carácter fragmentario significa que la ciencia penal solo debe sancionar algunas modalidades de conducta que lesionen o pongan en peligro bienes jurídicos”. (Salas Campos, 2001, p. 97).

Es por esto que el derecho penal solo sancionará aquellas conductas, ataques o comportamientos específicos; cuando sean los más peligrosos y repudiados por la sociedad.

Dependiendo el grado de ataque es como debe ser sancionado, es decir, que no todos aquellos ataques constituyen un delito, sino solamente los más peligrosos y que socialmente son más repudiados por la sociedad y que inciten una irritación o vallan en contra de la normalidad dentro de ésta.

El derecho penal como se mencionó solo protege los ataques más intolerables por la sociedad, “de lo contrario, si se sancionara cualquier ataque el país podría convertirse en un estado policiaco y se correría el riesgo de paralizar toda la actividad social; además los ciudadanos no podrían vivir bajo amenaza penal constante en todas

sus actividades sociales lo cual provocaría la consecuente inseguridad jurídica". (Salas Campos, 2001, p. 98).

Otras características del carácter fragmentario son, "que el ataque contra todos los bienes no se sanciona por igual, sino con distinta intensidad según la gravedad del daño, es por esto que el derecho penal se caracteriza más por lo no castigado que por lo castigado" (Salas Campos, 2001, p. 98).

Por otra parte, según "el derecho penal debe considerarse siempre como la última ratio legis. Por este término se entiende que ha de ser el último recurso que el derecho debe tener para proteger el orden jurídico, es decir, antes de aplicar una pena se deben agotar otros medios jurídicos, cuando así sea razonable.

Solamente cuando esos medios fallen, se podrá recurrir al derecho penal, aplicando una pena, como la última instancia, afectando a uno de los valores más preciados que es la libertad.

En cuanto a que el derecho penal es además de naturaleza subsidiaria, "esto significa que cuando basten otros medios jurídicos (como la aplicación de sanciones del derecho civil, del derecho administrativo o de sus otras ramas jurídicas), ha de retraerse el derecho penal secundario o subsidiariamente". (Salas Campos, 2001, p. 100).

Es decir que cuando no corresponda la aplicación y mucho menos punir una falta, se deberá aplicar otra ley, ya que no es lo mismo punir una acción que lesiones a la sociedad, que cometer una simple falta administrativa.

4.4. Determinación del estado cognoscitivo del sujeto activo como medida preventiva en el delito informático

En el Congreso Sobre Redacción de Legislación en Materia de Delitos Cibernéticos de la OEA (2004 27 de enero), se observó que dentro de las medidas preventivas que la autoridad debe de revisar para la comisión de un delito, se encuentra la existencia de determinado estado cognoscitivo respecto de cada uno de los elementos componentes de un delito, por ejemplo, las normas pueden exigir pruebas de que el autor del ilícito transmitió intencionalmente un comando determinado y que, en consecuencia, su conducta temeraria causó un daño a la información o al sistema computacional.

Los diversos ordenamientos jurídicos adoptan distintos estados cognoscitivos, si bien generalmente se los puede ubicar en tres categorías: los que se inclinan por la “intencionalidad”, los que optan por la “temeridad” y los que no exijan estado cognoscitivo alguno.

Otro punto que se debe tener en cuenta es el uso histórico que los ordenamientos jurídicos han impulsado al estado cognoscitivo al momento de decidir cuáles son los adecuados para ser incluidos en la tipificación de los delitos relativos a redes digitales.

En ciertos casos puede resultar difícil probar el estado cognoscitivo del acusado al momento en que ocurrió el acto.

Cuando la norma exija pruebas de que el infractor actuó intencionalmente, este requisito deberá restringirse a la demostración de que aquél tuvo la intención de ejecutar el acto en cuestión, en lugar de que su propósito fuera causar un daño emergente o una pérdida pecuniaria, por ejemplo, la ley podría exigir pruebas de que un delincuente tenía la intención de causar un daño mediante la interferencia o eliminación de los datos o la paralización de un sistema computacional, sin exigir la necesidad de que se demuestre que el infractor intentaba causar un perjuicio pecuniario específico.

4.4.1. Acceso de la autoridad a contenidos de la red

En el Congreso Sobre Redacción de Legislación en Materia de Delitos Cibernéticos de la OEA (2004 27 de enero), se observó que las redes computacionales generalmente permiten el almacenamiento de grandes cantidades de datos en sitios que se hallan alejados del lugar en que se encuentra la computadora de un usuario.

En el marco de la investigación de ilícitos, las autoridades deben contar con la autorización necesaria para obtener esos datos o para obligar al proveedor de servicios a revelarlos.

Esos datos pueden consistir en mensajes de correo electrónico que un cliente envió al proveedor de servicios de Internet.

De igual modo, muchas redes permiten el almacenamiento de los archivos del usuario en un servidor central de gran capacidad.

Si bien las normas legales que rigen el acceso a dicha información pueden ser similares a las que gobiernan el cateo o incautación de información que se encuentre en el domicilio de una persona, no hay necesidad de que sean idénticas, debido a una serie de consideraciones, dichas leyes pueden contener menos restricciones que las que rigen el cateo de espacios físicos.

En primer lugar, la persona física o jurídica que almacena y tiene acceso a los datos es en general un tercero neutral, como sucede en el caso de una empresa o proveedor de servicios que actúen en forma legal, en estos casos no se aplican los mecanismos coercitivos del proceso judicial tradicional, tales como la facultad de las autoridades de aplicación de justicia de ingresar a un domicilio por la fuerza y sin permiso, además la expectativa de privacidad de la información puede ser menor para aquellas personas que opten por entregar sus datos a un tercero para que los almacenen, en lugar de hacerlo en sus propios domicilios.

La facultad de acceder a la información almacenada en una red computacional es fundamental para la investigación de actos de delincuencia cibernética.

Es frecuente que dicha información haga las veces de escena del crimen en donde los investigadores buscarán pruebas de los elementos sustraídos, aspectos del modo de operar y posibles autores.

Del mismo modo que, en base a los métodos tradicionales de investigación, los agentes necesitan la facultad de recolectar pruebas o de obligar a personas físicas y jurídicas a que las proporcionen, deben asimismo contar con una autorización cuando se trate de pruebas en medios electrónicos, ya que sin ella sus tareas se verían gravemente coartadas.

El artículo 18 de la Convención sobre Delincuencia Cibernética del Consejo de Europa exige que los signatarios cuenten con leyes que confieran a los agentes del orden la posibilidad de acceder a la información alojada en redes de computadoras.

Aún en el caso de que no existan consideraciones significativas en materia de privacidad respecto de los datos almacenados en forma remota, los propietarios de los mismos mantienen una fuerte expectativa de que se respetará la confidencialidad.

Las empresas, gobiernos y ciudadanos utilizan cada vez más el formato electrónico para almacenar sus datos más confidenciales en servidores remotos, así el legislador deberá considerar la imposición de restricciones razonables a la facultad de acceso a esa información conferida a los agentes, teniendo en cuenta que dicha facultad sirve también para aumentar el nivel de privacidad como se ejerce a fin de investigar o procesar a los delincuentes que la violan al robar los datos confidenciales.

El Código Federal de Estados Unidos, confiere el grado más alto de protección a los mensajes de correo electrónico que se hallan almacenados para ser transmitidos, es

decir, aquellos que están en manos del proveedor de servicios y van en camino hacia su destino, por más que el receptor posiblemente no tenga conocimiento de su existencia, para interceptar esta categoría de datos almacenados, la ley exige una orden de cateo dictada por un juez, imponiendo además el requisito de que existan pruebas o elementos, que también se requieren en los casos de órdenes de allanamiento de domicilio.

Esta ley también dispone sanciones administrativas (como por ejemplo el descenso de rango y otras medidas disciplinarias) para aquellos investigadores que abusen de estas facultades, además de restricciones en cuanto a la revelación de la información obtenida mediante este mecanismo y la posibilidad de que inicien juicios civiles contra el estado por violación de las normativas del procedimiento.

Es de considerarse que todos los tipos de información almacenada merecen el mismo grado de protección, es por esto que, se deberá tener en cuenta a que instancias los proveedores de servicios, voluntariamente, podrán divulgar datos e información a las autoridades.

Por un lado, si estas revelaciones de información no tienen restricción alguna; puede llegar a constituir violaciones a la privacidad, especialmente en los casos en que las autoridades presionen a los proveedores con formas extraoficiales.

Por el otro, en ciertas circunstancias tiene sentido permitir que los proveedores de servicios de comunicación relativa a una amenaza a la salud o a la seguridad pública, al igual que aquella brindada a las autoridades a efectos de denunciar un ataque a la red del proveedor.

4.4.2. Acceso de la autoridad a información que no está almacenada en la red

En el Congreso Sobre Redacción de Legislación en Materia de Delitos Cibernéticos de la OEA (2004 27 de enero), se contempló que en general, las redes computacionales crean registros que indican quién las está utilizando, quiénes son los remitentes y destinatarios de las comunicaciones, y qué acciones se están ejecutando respecto de los programas informáticos y datos allí almacenados.

Si bien en muchas ocasiones estos registros son de importancia fundamental a la hora de resolver actos delictivos o terroristas cometidos a través de la red, el acceso a los mismos generalmente presenta menos inquietudes en materia de privacidad que el acceso al contenido de las comunicaciones subyacentes a ellos.

Por ejemplo, a efecto de individualizar un correo electrónico enviado a una conocida organización terrorista, si no interceptaron el mensaje o los datos de tráfico del mismo durante la transmisión (como sucede en la mayoría de los casos), los investigadores deberán recurrir a datos de tráfico almacenados, de igual modo si han identificado la cuenta que utilizan de un proveedor de servicios de Internet que está siendo usada para transmitir pornografía infantil, deberán entonces solicitar la revelación de los registros que indiquen el número telefónico que se utilizó para acceder a la cuenta.

Sólo con la facultad de obligar a que se efectúe la revelación de dichos registros podrán rastrear e individualizar al autor del ilícito.

Si bien las normas legales pueden disponer el tratamiento de todos los tipos de datos de tráfico, no es necesario que así ocurra, algunas clases de datos que no implican contenido suponen menos consideraciones en materia de privacidad que otras.

Por ejemplo, la norma podría distinguir entre la información básica del cliente de un proveedor de servicios de Internet (como por ejemplo su nombre, domicilio y método de pago) de los registros que muestran todas las actividades de realiza esa persona al

usar su cuenta (por ejemplo, quiénes le enviaron correos electrónicos y a quién dirigió mensajes de correo electrónico).

El Código Federal de EE.UU. realiza esta distinción, los investigadores pueden obtener información de identificación de una persona mediante un procedimiento judicial que solo requiere que la información sea relacionada a la investigación, aunque deben justificar ante un juez la necesidad de obtención de esos datos, indicando que existen hechos específicos que la ameritan.

Por último, un tema que debe tenerse en cuenta es la conservación de los registros, ya que las pruebas en medios electrónicos y en particular los registros que contienen datos de tráfico son de carácter temporal.

Los prestadores de servicios de comunicaciones generalmente no desean correr con los gastos de almacenar dicha información, y algunos ni siquiera llevan esos registros que pueden ser fácilmente eliminados en el curso ordinario de sus actividades lo que se diferencia de los delincuentes, que eliminan los registros en forma maliciosa.

No es inusual que los proveedores conserven los registros durante unos pocos días o semanas, además muchas veces los investigadores toman conocimiento del ilícito luego de que transcurrieron varios días o incluso semanas desde su comisión, por lo que probablemente el proveedor ya haya borrado la información que necesitan para rastrear las comunicaciones e individualizar al delincuente, aparte de todo esto, los procedimientos judiciales necesarios para obtener estos registros son generalmente bastante lentos.

La facultad de obligar al proveedor a conservar registros y demás datos relativos a una investigación penal (aunque no sea para revelarlos) es una herramienta que alivia la carga de investigación delictiva, dado que esas pruebas pueden destruirse con

mucha rapidez, la facultad debe ser ejercida expeditamente si ha de ser eficaz, sin que sea necesaria la aprobación de un juez.

Dicha aprobación se hace innecesaria, dado que son mínimas las inquietudes en materia de privacidad, debido a que no se revelará información alguna hasta en tanto se de cumplimiento al procedimiento judicial normal.

La solicitud de conservación de los datos sencillamente congela las pruebas a fin de que no desaparezca durante el lapso en que los investigadores cumplen con los procedimientos judiciales necesarios, sino se lograra dar razones por las cuales necesitaban la información o no pudiesen dar cumplimiento a los requisitos legales correspondientes, el proveedor no estará obligado a revelarles los mencionados datos.

El Código Federal de EE.UU. brinda un ejemplo de este tipo de disposición, mediante una simple solicitud escrita u oral, el investigador podrá pedir que el proveedor “tome todas las medidas necesarias a fin de conservar los registros y demás elementos de prueba que se hallen en su poder hasta en tanto se dicte una orden judicial o se cumpla con el procedimiento correspondiente”. La solicitud de conservación mantiene vigente la información por un plazo de 90 días, que puede ser programado.

4.4.3. Incautación de pruebas para quien es objeto de una investigación

En el Congreso Sobre Redacción de Legislación en Materia de Delitos Cibernéticos de la OEA (2004 27 de enero), se analizó la facultad necesaria para lograr un cateo o incautación de pruebas en medios electrónicos que se encuentren bajo el control de quien es objeto de una investigación.

En general, todos los países cuentan con leyes que permiten el cateo e incautación de documentos y objetos físicos que puedan servir de prueba de la comisión de un delito.

El legislador deberá considerar el grado de aplicación de esos mecanismos al mundo virtual, como sería el caso del cateo de pruebas intangibles (por ejemplo, datos almacenados en el disco duro de una computadora).

Las autoridades de aplicación de justicia necesitan la facultad de realizar cateos o incautaciones de computadoras y pruebas electrónicas que se hallen en manos de delincuentes. En el caso de ilícitos cometidos a través de Internet, por ejemplo, los investigadores generalmente se ven obligados a rastrear las comunicaciones hasta llegar a su punto de origen, una vez que se ha identificado la computadora que se halla en el domicilio o empresa en cuestión y desde la cual se enviaron las comunicaciones electrónicas sospechosas, se debe incautar para poder así confirmar las pistas que poseen e individualizar a quien las envió.

De esta manera, si se produce una intrusión a la computadora de una institución bancaria y se roban fondos, los investigadores deberán examinar los registros de la máquina, rastrear las comunicaciones hasta llegar a un proveedor de servicios de Internet y finalmente ubicar el lugar desde donde el pirata informático perpetró el delito.

Como paso final de la investigación, generalmente realizarán un cateo al lugar, incautarán la computadora o la información electrónica en ella alojada y arrestarán al delincuente.

El artículo 19 de la Convención sobre Delincuencia Cibernética del Consejo de Europa exige que los signatarios cuenten con normas que permitan que las autoridades efectúen dichas incautaciones.

4.4.4. Incautación de computadoras y datos electrónicos

En el Congreso Sobre Redacción de Legislación en Materia de Delitos Cibernéticos de la OEA (2004 27 de enero), se observó que en frecuentes ocasiones los investigadores deben incautar el soporte físico (hardware) de la computadora, lo que puede ser necesario, por ejemplo, a fin de proceder a su análisis en el laboratorio informático-forense debido a que la máquina contiene elementos ilegales, como es el caso de las imágenes de pornografía infantil, en estos casos la computadora debe ser tratada como cualquier otro objeto, aplicándole las normas que rigen la incautación de elementos probatorios físicos.

La cuestión es menos clara en aquellas instancias en las que los investigadores no tienen necesidad de incautar el soporte físico y sólo requieren copiar los archivos que se encuentran en la computadora, o incluso realizar una copia exacta de todo el dispositivo de almacenamiento electrónico, en estos casos no han procedido a quitar ningún objeto físico del lugar, ni privaron al propietario de su derecho de usar la información.

A primera vista parecería que estos elementos hacen que el acto sea menos invasivo o perjudicial respecto de los derechos del propietario, sin embargo, los datos almacenados en un domicilio o empresa pueden ser de carácter altamente confidencial, como sería el caso de un diario personal, de un testamento o de información de propiedad exclusiva o de naturaleza económico-empresarial, podría argumentarse en forma sólida, que toda esa información debería tratarse de forma similar, independientemente de que si se halla contenida copia impresa o en formato electrónico.

Así, el legislador deberá pensar en hacer normas sobre la copia de datos electrónicos para efectos de investigación para que sean equivalentes a las que rigen la incautación del soporte físico (hardware) que los contiene. La utilización de normas y

procedimientos aceptados otorga un equilibrio al proceso investigación, a la vez que le da un marco de certeza.

Claro está que si los investigadores cumplen la normativa aplicable, la copia de los datos en lugar de la incautación de la computadora debe considerarse un método permisible de cateo e incautación, además las excepciones a las normas tradicionales (quizá para aquellos casos en los que las autoridades cuenten con el permiso del propietario o cuando se trate de una emergencia de seguridad o de salud pública), deberán aplicarse también a la copia de datos para efectos de investigación o a la incautación del soporte físico de la computadora.

4.5. Aspectos jurisdiccionales en la comisión del delito informático

En el Congreso Sobre Redacción de Legislación en Materia de Delitos Cibernéticos de la OEA (2004 27 de enero), se señaló que dado que las redes internacionales carecen de fronteras, un único acto delictivo ejecutado mediante el uso de una computadora puede llegar a afectar a varios países.

Cada vez con más frecuencia los piratas informáticos atacan computadoras que se hallan en países distintos de los suyos, incluso aún cuando su fin último sea acceder en forma no autorizada a una computadora que se encuentra en su país de residencia, generalmente ingresan primero a sistemas ubicados en el extranjero, utilizándolos como sistemas intermedios o como campo de preparación para atacar desde allí a sus verdaderos objetivos.

Este proceso, es conocido como “looping” y les permite ocultar sus identidades, además de ser sumamente sencillo de poner en práctica, genera una pesada carga en lo que respecta a acciones de cooperación internacional entre autoridades.

La creciente incidencia del pirateo informático internacional y del proceso de “looping”, que los infractores usan a fin de ocultar sus identidades, ha obligado a que los ordenamientos jurídicos sean creativos en la adaptación de sus normativas.

Algunos países, por ejemplo, han vuelto a analizar sus políticas y leyes en materia de extradición a efecto de asegurarse que no existan naciones que sirvan de refugio para los piratas informáticos. Además, si un delincuente informático de un país ingresa ilegalmente a las computadoras de los bancos de otras naciones, parece tener más sentido que los derechos de las víctimas internacionales sean reivindicados mediante el procesamiento judicial del infractor en el país de origen de éste, en lugar de emprender acciones judiciales separadas en contra del mismo en cada una de las naciones en las que cometió el ilícito.

A modo de ejemplo podemos indicar que si bien el gusano Nimda causó daños a computadoras en casi todos los países del mundo, tendría poco sentido que quien lo lanzó fuese sometido a juicios y sanciones repetidas veces.

Todos los países deben contar, al menos, con el grado máximo de flexibilidad posible para procesar a piratas informáticos ubicados dentro y fuera de sus fronteras.

En particular, las leyes internas deben penalizar los ataques a las computadoras que se hallen dentro del país, independientemente de que el infractor se encuentre dentro o fuera del territorio del mismo, al mismo tiempo las normas de cada país deben prever el procesamiento de los delincuentes internos que ataquen computadoras ubicadas en el exterior.

En el caso de que no esté disponible ese mecanismo de procesamiento interno, los tratados y normas legales del país en cuestión deberán disponer la extradición a la nación en la que se encuentra la víctima del delito, además, las normas procesales deben servir de respaldo para la investigación y procesamiento de personas que se

encuentren en el extranjero, permitiendo la recolección e intercambio de pruebas del delito entre las autoridades de procuración y administración de justicia.

El ordenamiento jurídico australiano contiene un ejemplo de la primera de las normas mencionadas, esta ley confiere a las autoridades australianas la competencia necesaria para procesar a todo delincuente que ataque computadoras ubicadas en ese país, independientemente del lugar en el que se halle el infractor, de igual modo, en EE.UU. una reciente modificación legislativa permite que sus fiscales impongan cargos penales contra extranjeros que ataquen computadoras de su país, como así también contra todo estadounidense que perpetre tales actos en computadoras de otros países.

Esta ley otorga un beneficio adicional, ya que confiere a los investigadores estadounidenses la competencia necesaria para examinar las intrusiones efectuadas en computadoras extranjeras, lo cual significa que pueden abrir rápidamente una investigación, además de obtener pruebas en forma más expedita y compartirlas con los demás países.

La Convención sobre Delincuencia Cibernética de 2001 del Consejo de Europa contiene la siguiente disposición en materia jurisdiccional:

Artículo 22. – Jurisdicción

1. Cada una de las partes adoptará las medidas legislativas y de otra naturaleza que sean necesarias a fin de establecer jurisdicción respecto de actos ilícitos....cuando el ilícito:

    a. se cometa en su territorio; o

    b. se cometa a bordo de un buque que lleve la bandera de la parte de que se trate; o

c. se cometa a bordo de una aeronave registrada con arreglo a las leyes de dicha parte; o

d. sea cometido por una persona con la nacionalidad de la Parte, en el caso de que el ilícito sea punible por la ley penal del lugar en que fue cometido o cuando sea cometido fuera de la jurisdicción territorial de un Estado.

2. Cada una de las partes adoptará las medidas legislativa y de otra naturaleza que sean necesarias a fin de establecer jurisdicción respecto de actos ilícitos previstos en el Artículo 24 (1) de la presente Convención, en los casos en que el presunto infractor se halle presente en su territorio y no se proceda a su extradición a otra parte, sólo en razón de la nacionalidad del mismo, luego de haberse efectuado un pedido de extradición.

3. En el supuesto de que más de una Parte alegue tener jurisdicción respecto de un presunto ilícito, conforme lo establecido en la presente Convención, las partes en cuestión, de corresponder, deberán realizar consultas con vistas a determinar la jurisdicción más adecuada para el procesamiento judicial del ilícito.

4.5.1. Determinación de la pena adecuada

En el Congreso Sobre Redacción de Legislación en Materia de Delitos Cibernéticos de la OEA (2004 27 de enero), se indicó que existen muchas normas de penalización de delitos cometidos en redes digitales como países que las han sancionado, si bien no hay una única respuesta correcta a la pregunta cuan severa debe ser la pena aplicada a los delitos descritos en el presente documento, el legislador debe establecer sanciones que sean lo suficientemente serias como para disuadir y castigar toda

invasión de la privacidad, robo de información y daños pecuniarios o de otra naturaleza que resulten de una conducta ilícita.

Los mecanismos de disuasión y sanción generalmente incluyen multas, penas de prisión por plazos significativos y actos de restitución a las víctimas.

4.5.2. Daños pecuniarios

En el Congreso Sobre Redacción de Legislación en Materia de Delitos Cibernéticos de la OEA (2004 27 de enero), un criterio importante que se observó es: para determinar la gravedad de la sanción correspondiente a un delito en particular consistente en examinar el daño o pérdida pecuniaria que ha causado, la norma debe tener en cuenta todos los costos incurridos en el descubrimiento de la intrusión, la determinación de su alcance y el tiempo y recursos utilizados en la restauración de la computadora y de los datos de su estado original. Esta cifra debe también incluir el tiempo utilizado por los empleados a fin de reparar el sistema (utilizándose al efecto el costo por hora de su sueldo), así como también la pérdida de productividad debido a la inoperatividad de la computadora.

Por ejemplo, en el supuesto de que un intruso ingrese ilegalmente a la red y elimine los registros de la base de datos, causando la caída del sistema, la pérdida pecuniaria podría incluir los siguientes conceptos:

El costo de detectar e investigar la intrusión, el costo de individualizar los datos que quedaron corrompidos por la intrusión, el costo de restaurar los datos que quedaron corrompidos por la intrusión, el costo de restaurar los datos utilizando una copia de seguridad, el costo de recrear los datos perdidos, la pérdida de ventas causadas por la caída del sistema, la pérdida de productividad debido a que los empleados se vieron imposibilitados de realizar sus tareas, el costo de reforzar el mecanismo de seguridad

del sistema a fin de garantizar que el intruso no haya dejado una “puerta trasera” que le permita volver a acceder a él en forma no autorizada.

De lo anterior también deberá incluirse la pérdida resultante de la caída del buen nombre comercial y reputación de la empresa, en el caso de que un especialista lo pueda calcular.

Dependiendo del tipo de acto ejecutado durante la intrusión, el delito puede causar otros perjuicios pecuniarios cuantificables, por ejemplo, si un pirata informático ingresa ilegalmente a una computadora a efecto de darle un uso personal (como sucedería si accede a una supercomputadora para utilizar su potencia a fin de correr sus propios programas) el daño pecuniario deberá incluir el valor del tiempo de uso del sistema, aparte de los gastos de investigación y reparación.

De igual forma, si el intruso roba información, deberá incluirse el valor de la misma en la cifra total que se calcule como pérdida, si la información tenía un valor inherente, como sucedería en el caso de que sea ella misma el objeto de comercialización, el juez podrá determinar fácilmente dicho valor.

Si se trata de datos de propiedad exclusiva, por ejemplo determinadas fórmulas industriales, el juez deberá quizá determinar el daño pecuniario intentando establecer el valor que tiene esa información para la empresa.

Esta cuestión puede también analizarse examinando los beneficios que obtuvo el intruso, sean estos económicos o de cualquier otra naturaleza, por ejemplo, si obtuvo datos relativos a un proceso de producción secreto y los vendió a la competencia por una suma de dinero, el juez podría determinar que esa cifra corresponde al valor real de la información en cuestión.

La falta de beneficio personal no debe ser causal de eliminación de la pena, muchos piratas informáticos ingresan ilegalmente a los sistemas sencillamente para probar que podían hacerlo, o bien para aumentar su reputación, sin buscar beneficio económico alguno.

Por último, la norma debe también considerar que una única intrusión o una serie de intrusiones efectuadas por un pirata informáticos pueden afectar a muchas computadoras, causando daños y pérdidas monetarias a cada uno de sus propietarios.

Al mismo tiempo, la evaluación del daño causado a cada una de las computadoras de la red puede ser más difícil que el cálculo de perjuicio pecuniario total que sufrió el propietario del sistema, por ejemplo, el caso de un intruso que compromete la red de una pequeña empresa que cuenta con 40 computadoras, alterando los datos de solo 5 de ellas y paralizando a otras 5.

Para la empresa puede ser fácil calcular la pérdida total sufrida, pero quizá le sea difícil repartir el daño a cada una de las computadoras, por esto la norma debe permitir que el juez sume los daños causados a varias computadoras durante el curso del acto delictivo.

Existen varias razones por las cuales los mencionados métodos de cálculo de pérdidas pecuniarias debidas a un ilícito informático no sirven para dar adecuada cuenta de la gravedad del delito.

En primer lugar, los efectos reales de la intrusión pueden ir mucho más allá de la red afectada y causar daños pecuniarios no cuantificables en forma inmediata, un aspecto aún más importante es que muchos de los perjuicios emergentes de los delitos cometidos en redes generan otras clases de daños a la sociedad que no pueden ser evaluados en términos monetarios.

4.5.3. Amenazas a la seguridad pública y daños a infraestructuras nacionales de importancia crítica

En el Congreso Sobre Redacción de Legislación en Materia de Delitos Cibernéticos de la OEA (2004 27 de enero) se analizó y se reconoció que en muchos países su infraestructura de importancia crítica depende cada vez más de las computadoras.

Las infraestructuras de importancia crítica son aquellas que mantienen el funcionamiento básico de una economía, como ocurre con los sistemas bancarios, financieros, de telecomunicaciones, de transporte, de emergencia, de atención médica y de distribución de energía, agua y alimentos.

Los daños a estas infraestructuras tienen importantes consecuencias económicas, además de configurar una amenaza a la seguridad pública.

Las computadoras juegan un papel cada vez más decisivo en la prestación de estos importantes servicios, lo cual significa que son vulnerables a las nuevas formas de ataque cibernético.

Es por esto que las leyes sobre delitos cometidos en redes digitales deben prever sanciones graves a toda conducta que amenace con perturbar dichas infraestructuras, aunque esos perjuicios no siempre puedan traducirse fácilmente en términos pecuniarios.

CONCLUSIONES

En los primeros años del siglo XX se da un sorprendente avance de la tecnología, por el descubrimiento de nuevos dispositivos electrónicos, dándose así, la creación de una herramienta que vino a solucionar los problemas del ser humano y simplificar su trabajo, por su gran capacidad de almacenamiento de información, siendo ésta la computadora.

Las redes proporcionan apoyo a actividades de infraestructuras de importancia en el campo de la energía, el transporte, áreas bancarias y financieras que desempeñan un papel importante en las actividades de las empresas y en los mecanismos de prestación de servicios que el estado proporciona a los ciudadanos y a la comunidad empresarial, además de servir como medio de intercambio de información y comunicación.

Es preocupante que los avances tecnológicos abran la posibilidad a actividades delictivas, debido a esto la necesidad de intensificar los esfuerzos para combatir los abusos relacionados con la informática, cubriendo las lagunas que permiten a los delincuentes poder actuar impunemente, estableciendo de forma clara y precisa conceptos básicos incluyendo derechos y obligaciones lo cual permitirá tipificar cada una de las conductas y sancionarlas de acuerdo a su gravedad, ayudando a regular la actividad informática y su convivencia pacífica con el derecho.

El hecho de que Internet no tenga fronteras facilita a las personas a cometer ilícitos sin mostrar su rostro, éste tipo de delincuentes, son personas decididas, listas, con conocimiento de la tecnología, dispuestas a aceptar retos y con cierto estatus socioeconómico y debido a sus características se les denomina, “delincuentes de cuello blanco”, mismos que se escudan dentro de las conductas no tipificadas por la ley como delitos para cometer sus ilícitos, como por ejemplo, violación a las leyes de patentes y derechos de autor, el mercado negro, evasión de impuestos, narcotráfico, contrabando, pornografía infantil, entre otros.

Internet es un medio por el cual podemos manifestar libremente las ideas, informar y comunicar, pero se encuentra sujeto a las limitaciones impuestas por el artículo 6º constitucional, es decir, que siempre y cuando no ataque a la moral, los derechos de terceros ni provoque algún delito o perturbe el orden público, cosa que no se da debido a los múltiples temas que pueden encontrarse dentro de la red, enfrentándonos a un gran problema.

La regulación de Internet no se ha realizado, es por eso que se rige solo por códigos éticos y la tendencia que se observa es que será un fenómeno autorregulable, pero bien sabemos que falta mucho debido a la complejidad de compaginar las leyes locales con el mundo de la red, empezando por que dentro de nuestra legislación no se reconoce el termino Internet y lo interpreta solo como un concepto de valor agregado, esto trae como consecuencia que surjan problemas como la violación a la intimidad divulgación de información privada e intima, dando como resultado la propagación de números de tarjetas de crédito, registros financieros, médicos, a través de Internet, por grupos de piratas informáticos que ingresan ilegalmente a bases de datos robando información y ocasionando grandes daños.

Internet es utilizado para cometer toda clase de acciones antijurídicas, mismas que se encuentran plasmadas en códigos y leyes pero no enfocados en la materia informática, es por eso que se recurre a la analogía, la cual no se aplica en la materia penal, quedando impunes muchos ilícitos.

Es urgente ampliar y actualizar nuestra legislación a todos los niveles debido a que Internet se ha convertido hoy en día en una herramienta importantísima para el desarrollo de un país, con esto no se pretende descubrir algo nuevo sino solo mostrar lo que es evidente, que se necesita un análisis profundo para evitar que se sigan utilizando a los medios informáticos, como medios de comisión de delitos y se salvaguarden bienes jurídico de importancia para la sociedad.

Los delitos informáticos constituyen un gran reto para todos los sectores de un país así como para legisladores, instituciones policiales, encargadas de las investigaciones, jueces y magistrados, los cuales tienen la tarea de crear una legislación que sancione toda conducta que amenace o perturbe el bien común y la convivencia pacífica de un país.

BIBLIOGRAFÍA

Leyes y Reglamentos:

Código Penal Federal. México: Ediciones Libuk S.A. de C.V.

Código Penal para el Distrito Federal. México: Ediciones Libuk S.A. de CV.

Constitución Política de los Estados Unidos Mexicanos. México: Editorial Sista, S.A. de C.V.

Convención sobre delitos cibernéticos del consejo de Europa. 2001

Explicación de la convención sobre delitos cibernéticos del consejo de Europa, 2001

Leyes de Estados Unidos Criminalizando los Ataques a la Red de Computadoras y Regulando la Colección de Evidencia Electrónica.

Resolución 55-63 de la asamblea general de la ONU. (Lucha contra la utilización de la tecnología de la información con fines delictivos).2000

Fuentes Bibliográficas:

BARRIOS GARRIDO Gabriela, et al; Internet y el derecho en México, editorial Mc Graw Hill, 1998.

CAMPOLI Gabriel Andrés, Delitos Informáticos en la Legislación Mexicana, editorial Instituto Nacional de Ciencias Penales, 2005.

DEL POZO Luz Maria y Ricardo HERNANDEZ, Informática en Derecho, editorial Trillas, 1992.

DE PINA VARA Rafael, Diccionario de Derecho, editorial, Porrúa, 1998.

DION MARTINEZ Carlos; Curso de lógica, 2ª edición, editorial Mc Graw Hill, 1976.

FERNANDEZ DELPECH Horacio; Internet: su Problemática Jurídica; editorial Abeledo-Perrot, 2001.

FERREIRA CORTES Gonzalo, Informática Paso a Paso, editorial. Alfaomega, 2004.

FLORES GÓMEZ GONZÁLEZ Fernando y Gustavo CARVAJAL MORENO, Nociones de Derecho Positivo Mexicano, 31ª Edición, editorial Porrúa, 1992

KEENAN Forsythe y Organick STEMBERG, Lenguajes de Diagrama de Flujo, editorial Limusa, 1981.

Inventos que Cambiaron el Mundo, Diccionario, editorial, Selecciones de Reader`s Digest, 1983.

LITLETON ZINDER Dedra, Prevención y Detención del Delito Informático, editorial Anaya multimedia, 2002.

M. COPI Irving; Lógica simbólica; 16ª edición, editorial CECSA, 1998.

MOLINA SALGADO Jesús Antonio, Delitos y Otros Ilícitos Informáticos en el Derecho de la Propiedad Industrial, editorial Porrúa, 2003.

NANDO LEFORT Víctor Manuel, El Lavado de Dinero, editorial Trillas, 1997.

NORTON Peter, Introducción a la Computación, editorial Mc. Graw Hill, 2006.

OLEA FRANCO Pedro, Manual de Técnicas de Investigación Documental, 21ª Edición, editorial Esfinge, 1992.

OROZCO GOMEZ Javier; El marco jurídico de los medios electrónicos, editorial Porrúa, 2001.

OSORIO Y NIETO Cesar Augusto, Delitos Federales, editorial Porrúa, 2005.

ROJAS SORIANO Raúl, Guía para Realizar Investigaciones Sociales, editorial PyV, 3ª Edición, 1989.

SALAS CAMPOS Raúl, La teoría del Bien Jurídico en el Derecho Penal, editorial, Oxford.

TÉLLEZ VALDÉS Julio, Derecho Informático, 3ª Edición, editorial Mc. Graw Hill, 2004.

VASCONCELOS SANTILLÁN Jorge, Introducción a la Computación, editorial Publicaciones cultural, 1997.

VILLALOBOS Laura Elena, Introducción a la Computación y Manejo ms-dos, editorial Universidad Nacional Autónoma de México, 1991.

V. CASTRO Juventino, Garantías y Amparo, editorial Porrúa.

Fuentes Electrónicas:

Legislación Sobre Delitos Informáticos, http//www.monografias.com

Delitos Informáticos, http://derpeninformatico.tripod.com/principal.html
http://www.ejournal.unam.mex/boletin_mderecho/Bolmex109/BMD10903.pdf

http://www.monografias.com/trabajos23/bien-juridico/bien-juridico.shtml#delitos

http://www.vecam.org/article659.html

http://www.laflecha.net/articulos/seguridad/delito_informatico/

http://www.delitosinformaticos.com/delitos/delitosinformaticos.shtml

http://www.segu-info.com.ar/delitos/informacionydelito.htm

http://www.davara.com/preguntas/delitos.html#3

http://www2.netexplora.com/biblioteca/netiquettes.html

http://pakavenue.com/webdigest/it_corner/intro_006.htm

http://www.isocmex.org.mx/kiyoshi.html

http://espanol.news.yahoo.com/s/06062007/4/negocios-falta-regulaci-n-internet-fuente-delitos-l-nea-experto.html

GLOSARIO

Cibernética: Es la ciencia de la comunicación y el control.

Informática: Conjunto de técnicas destinadas al tratamiento lógico y automatizado de la información para una adecuada toma de decisiones.

Computadora: Es una máquina electrónica que permite el pensamiento o procesamiento de datos y emite un resultado.

Red: es un grupo de computadoras y periféricos conectados físicamente y un vasto número de programas especializados para permitir el intercambio de datos y compartir los recursos instalados.

Virus: Son pequeños programas que dañan o borran la información que contiene una computadora.

Derecho de la información: Conjunto de leyes, normas y principios aplicables a los hechos y actos derivados de la informática.

Informática Jurídica: Es la técnica interdisciplinaria que tiene por objeto el estudio e investiga la informática general, aplicable a la recuperación de análisis y tratamientos jurídicos.

Internet: Es una red global de redes de ordenadores cuya finalidad es permitir el intercambio libre de información entre todos sus usuarios.

Delitos Informáticos: Actos ilícitos en que se tiene a las computadoras como instrumento o fin.

Amenaza informática: es cualquier cosa que pueda ocasionar daños a un equipo de cómputo.

Información Privada: Es aquella sobre la cual el titular posee un derecho exclusivo de uso o conocimiento pero que en mayor o menor medida es conocida por un grupo de personas a su alrededor y por el estado respondiendo a fines de garantía de los derechos del ciudadano.

Información íntima: Es aquella sobre la cual el titular tiene la absoluta exclusividad de su conocimiento y divulgación, que se encuentra ligada a sus procesos internos de selección y no puede ser conocida ni aun en circunstancias especiales por persona alguna ni por el estado.

Crimen cibernético: es cualquier acto criminal que se realice a través de una computadora.

Hacker: es una persona que goza, alcanzando un conocimiento profundo sobre el funcionamiento interno de un sistema, de una computadora o de una red de computadoras.

Cracker: Es una persona que intenta acceder a un sistema informático con malas intenciones, sin autorización.

CONCLUSIONES

En los primeros años del siglo XX se da un sorprendente avance de la tecnología, por el descubrimiento de nuevos dispositivos electrónicos, dándose así, la creación de una herramienta que vino a solucionar los problemas del ser humano y simplificar su trabajo, por su gran capacidad de almacenamiento de información, siendo esta la computadora.

Estas nuevas tecnologías de información y comunicación deben de ir de la mano con el mundo jurídico, debido a que es necesaria una regulación que ayude a comprender el estudio de esta materia, ya que recordemos que donde hay sociedad existe el derecho y un cuerpo de leyes que lo regula, no importando que se realice dentro de un mundo virtual de grandes redes de información.

Las redes proporcionan apoyo a actividades de infraestructuras de importancia en el campo de la energía, el transporte, áreas bancarias y financieras que desempeñan un papel importante en las actividades de las empresas y en los mecanismos de prestación de servicios que el estado proporciona a los ciudadanos y a la comunidad empresarial, además de servir como medio de intercambio e información y comunicaciones.

La información que se transmite es de gran importancia, por tal razón los sistemas y redes de información quedan expuestas a un gran número de amenazas, ni el comercio electrónico ni los mercados podrían desarrollarse sin redes de información sólidas y seguras que cuenten con la confianza del público.

Debido a lo anterior podemos decir que un elemento importante que sirve para garantizar la existencia de redes seguras consistente en un amplio marco jurídico

que logre actuar como factor disuasivo a las amenazas y ataques a redes, además de poder individualizarlos y procesar judicialmente a quien lo ocasione.

Es preocupante que los avances tecnológicos abran la posibilidad a actividades delictivas, debido a esto la necesidad de intensificar los esfuerzos para combatir los abusos relacionados con la informática, cubriendo las lagunas que permiten a los delincuentes poder actuar impunemente, estableciendo de forma clara y precisa conceptos básicos incluyendo derechos y obligaciones lo cual permitirá tipificar cada una de las conductas y sancionarlas de acuerdo a su gravedad, ayudando a regular la actividad informática y su convivencia pacifica con el derecho.

Las amenazas a las que nos encontramos expuestos pueden ser de distintos tipos, desde accesos ilegales hasta la contaminación de redes por programas dañinos produciendo un retroceso dentro de la economía de un país, dichos ataques son provocados por los hackers, crackers y ciberpiratas, mismos que vienen a romper con el esquema de a tecnología.

Tengamos en cuenta que el hecho de que Internet no tenga fronteras facilita a las personas a cometer ilícitos sin mostrar su rostro, éste tipo de delincuentes, son personas decididas, listas, con conocimiento de la tecnología, dispuestas a aceptar retos y con cierto estatus socioeconómico y debido a sus características se les denomina, “delincuentes de cuello blanco”, mismos que se escudan dentro de las conductas no tipificadas por la ley como delitos para cometer sus ilícitos, como por ejemplo, violación a las leyes de patentes y derechos de autor, el mercado negro, evasión de impuestos, narcotráfico, contrabando, pornografía infantil, entre otros.

Es importante que se tome en cuenta que dentro del mundo virtual no se permitan actos prohibidos en el mundo físico, debido a que los daños cometidos

por estos delincuentes pueden ser incalculables, así como también tomar mediadas para protegernos frente a amenazas, como por ejemplo el respaldar siempre nuestra información y cuidarla sobre todo la personal, para evitar el robo de identidad entre otros.

En cuanto a la manifestación de ideas podemos decir que Internet es un espacio que se caracteriza en este sentido, solo que también se encuentra sujeto a las limitaciones impuestas por el articulo 6º es decir que siempre y cuando no ataque a la moral, los derechos de terceros ni provoque algún delito o perturbe el orden público, cosa que no se da debido a los múltiples temas que pueden encontrarse dentro de la red, enfrentándonos a un gran problema, ya que para algunos algo que es inmoral para otros no lo es.

Es por esto que se insiste en la claridad dentro de las normativas que nos regulan y no basarnos en la interpretación, lo cual evitara problemas a los agentes encarados de realizar una investigación

La regulación de Internet no se ha realizado, es por eso que se rige solo por códigos éticos y la tendencia que se observa es que será un fenómeno autorregulable, pero bien sabemos que falta mucho debido a la complejidad de compaginar las leyes locales con el mundo de la red, empezando por que dentro de nuestra legislación no se reconoce el termino Internet y lo interpreta solo como un concepto de valor agregado.

La falta de regulación da como consecuencia que surjan problemas como la violación a la intimidad, la cual violenta la privacidad de secretos divulgándolos a través de nuevas tecnologías por grupos de piratas informáticos que ingresan ilegalmente a bases de datos robando información y ocasionando grandes daños.

La información privada también corre el mismo peligro solo que esta es conocida solo por algunas personas o por el estado, por ejemplo tarjetas de crédito, registros financieros, médicos, pero que si es conocida por la persona equivocada ocasiona daños, en cambio la información intima exclusiva nadie puede tener conocimiento de ella, incluyendo al estado, y mucho menos divulgarla pero que igual mete ocasiona daños al hacer publica la información.

Por otra parte como ya se menciono en Internet se dan en gran medida los intercambios culturales haciendo que surjan códigos de ética los cuales fungen como modelos jurídicos no escritos, lo cual no es lo mismo y un ejemplo de esto son las nettiquett, (etiqueta de la red, ciberetiqueta, ciberurbanidad), estas crean un conjunto de normas no dictadas por la costumbre, experiencia y sentido común, definiendo reglas de urbanidad que deben seguir usuarios en Internet, obviamente esto deja muchos temas en el aire y no regula situaciones mas complejas dentro de Internet.

Por esta razón Internet es utilizado para cometer toda clase de delitos, mismos que se encuentran plasmados en códigos y leyes pero no enfocados en la materia informática, es por eso que se recurre a la analogía, la cual no se aplica en la materia penal, quedando impunes muchos delitos, o en el mejor de los casos tratar de ingresarlo a otro tipo de delito como el fraude, derechos de autor o daños mismos que se persiguen civilmente.

Para tratar de dar una solución a este problema, en algunos estados se ha intentado legislar sobre el tema, pero lo que hemos podido observar es que en algunos casos la misma legislación que esta plasmada dentro de los códigos es la misma en otro estado, en otros casos es muy escasa y deja desprotegidas otros puntos importantes o se utilizan términos mal empleados, talvez por el desconocimiento del tema.

Como podemos ver no es cualquier tema por eso es urgente ampliar y actualizar nuestras legislaciones a todos niveles debido a que Internet se a convertido hoy en día en una herramienta importantísima para el desarrollo de un país, con esto no se pretende descubrir algo nuevo sino solo mostrar lo que es evidente, que se necesita un análisis profundo para evitar que se siga utilizando a los medios informáticos, como medios de comisión de delitos y salvaguardar el bien jurídico, que representa los valores e intereses de toda persona.

También es importante que dentro de la legislación se tomen en cuenta las sanciones las cuales deberán castigar las conductas que lesionen o pongan en peligro el bien jurídico, dependiendo por su grado evitando una amenaza penal constante dentro de la sociedad, dejando como ultimo recurso la aplicación de una pena afectando el bien jurídico mas preciado como lo es la libertad.

Para la determinación de la pena debemos tomar en cuenta el estado cognoscitivo en el que se encuentre el sujeto es decir si este tuvo la intención o no para cometer el ilícito, así como también el facilitar y capacitar a la autoridad proporcionando todas las facilidades para realizar su función, sin sobre pasar y abusar de sus facultades así como también la restricción de revelación de información.

Es importante que dentro de los países exista una espíritu de cooperación debido a la falta de fronteras en las redes internacionales ya que esto facilita a los delincuentes cometer delitos desde países lejanos, afectando a varios países, creando mecanismos como tratados y normas locales que permitan la extradición del delincuente al país que fue victima del ilícito.

Los delitos informáticos constituyen un gran reto para todos los sectores de un país así como para legisladores, instituciones policiales, encargadas de las investigaciones, jueces y magistrados, los cuales tienen la tarea de crear una

legislación que sancione toda conducta que amenace o perturbe el bien común y la convivencia pacifica de un país.

BIBLIOGRAFÍA

Leyes y Reglamentos:

Código Penal Federal. México: Ediciones Libuk S.A. de C.V.

Código Penal para el Distrito Federal. México: Ediciones Libuk S.A. de CV.

Constitución Política de los Estados Unidos Mexicanos. México: Editorial Sista, S.A. de C.V.

Convención sobre delitos cibernéticos del consejo de Europa. 2001

Explicación de la convención sobre delitos cibernéticos del consejo de Europa, 2001

Leyes de Estados Unidos Criminalizando los Ataques a la Red de Computadoras y Regulando la Colección de Evidencia Electrónica.

Resolución 55-63 de la asamblea general de la ONU. (Lucha contra la utilización de la tecnología de la información con fines delictivos).2000

Fuentes Bibliográficas:

BARRIOS GARRIDO Gabriela, MUNOSS DE ALBA M. Marcia, PEREZ BUSTILLO Camilo; Internet y el derecho en México; editorial Mc Graw Hill 1998.

CAMPOLI Gabriel Andrés, Delitos Informáticos en la Legislación Mexicana, editorial Instituto Nacional de Ciencias Penales, 2005.

DEL POZO Luz Maria y HERNÁNDEZ Ricardo, Informática en Derecho, editorial Trillas, 1992.

DE PINA VARA Rafael, Diccionario de Derecho, editorial, Porrua, 1ª Edición, 1998.

DION MARTINEZ Carlos; Curso de lógica, 2ª edición, editorial Mc Graw Hill 1976.

FERNANDEZ DELPECH Horacio; Internet: su Problemática Jurídica; editorial Abeledo-Perrot, 2001.

FERREIRA CORTES Gonzalo, Informática Paso a Paso, edit. Alfaomega, 2004.

FLORES GÓMEZ GONZÁLEZ Fernando y Carvajal Moreno Gustavo, Nociones de Derecho Positivo Mexicano, editorial Porrúa, 31ª Edición, 1992.

KEENAN Forsythe y STEMBERG Organick, Lenguajes de Diagrama de Flujo, editorial Limusa, 1ª Edición, 1981.

Inventos que Cambiaron el Mundo, Diccionario, editorial, Selecciones de Reader`s Digest, 1ª Edición, 1983.

LITLETON ZINDER Dedra, Prevención y Detención del Delito Informático, editorial Anaya multimedia, 2002

M. COPI Irving; Lógica simbólica; 16ª edición, editorial CECSA 1998.

MOLINA SALGADO Jesús Antonio, Delitos y Otros Ilícitos Informáticos en el Derecho de la Propiedad Industrial, Editorial Porrúa, 1ª Edición, 2003.

NANDO LEFORT Víctor Manuel, El Lavado de Dinero, editorial Trillas, 1997.

NORTON Peter, Introducción a la Computación, editorial. Mc. Graw Hill, 2006

OLEA FRANCO Pedro, Manual de Técnicas de Investigación Documental, editorial, Esfinge, 21ª Edición, 1992.

OROZCO GOMEZ Javier; El marco jurídico de los medios electrónicos, editorial Porrúa, 2001.

OSORIO Y NIETO Cesar Augusto, Delitos Federales, editorial Porrúa, 2005.

ROJAS SORIANO Raúl, Guía para Realizar Investigaciones Sociales, editorial, PyV, 3ª Edición, 1989.

SALAS CAMPOS Raúl; La teoría del Bien Jurídico en el Derecho Penal, editorial, Oxford.

TÉLLEZ VALDÉS Julio, Derecho Informático, Editorial. Mc. Graw Hill, 3ª Edición, 2004.

VASCONCELOS SANTILLÁN Jorge, Introducción a la Computación, editorial Publicaciones cultural, 1ª Edición, 1997.

VILLALOBOS Laura Elena, Introducción a la Computación y Manejo ms-dos, editorial Universidad Nacional Autónoma de México, 1ª Edición, 1991.

V. CASTRO Juventino, Garantías y Amparo, editorial, Porrúa.

Fuentes Electrónicas:

Legislación Sobre Delitos Informáticos, http//www.monografias.com.

Delitos Informáticos, http://derpeninformatico.tripod.com/principal.html.

http://www.ejournal.unam.mex/boletin_mderecho/Bolmex109/BMD10903.pdf

http://www.monografias.com/trabajos23/bien-juridico/bien-juridico.shtml#delitos

http://www.vecam.org/article659.html

http://www.laflecha.net/articulos/seguridad/delito_informatico/

http://www.delitosinformaticos.com/delitos/delitosinformaticos.shtml

http://www.segu-info.com.ar/delitos/informacionydelito.htm
http://www.davara.com/preguntas/delitos.html#3

http://www2.netexplora.com/biblioteca/netiquettes.html

http://pakavenue.com/webdigest/it_corner/intro_006.htm

http://www.isocmex.org.mx/kiyoshi.html

http://espanol.news.yahoo.com/s/06062007/4/negocios-falta-regulaci-n-internet-fuente-delitos-l-nea-experto.html

GLOSARIO

Cibernética: Es la ciencia de la comunicación y el control.

Informática: Conjunto de técnicas destinadas al tratamiento lógico y automatizado de la información para una adecuada toma de decisiones.

Computadora: Es una máquina electrónica que permite el pensamiento o procesamiento de datos y emite un resultado.

Red: Es un grupo de computadoras y periféricos conectados físicamente y un vasto número de programas especializados para permitir el intercambio de datos y compartir los recursos instalados.

Virus: Son pequeños programas que dañan o borran la información que contiene una computadora.

Derecho de la información: Conjunto de leyes, normas y principios aplicables a los hechos y actos derivados de la informática.

Informática Jurídica: Es la técnica interdisciplinaria que tiene por objeto el estudio e investiga la informática general, aplicable a la recuperación de análisis y tratamientos jurídicos.

Internet: Es una red global de redes de ordenadores cuya finalidad es permitir el intercambio libre de información entre todos sus usuarios.

Delitos Informáticos: Actos ilícitos en que se tiene a las computadoras como instrumento o fin.

Amenaza informática: es cualquier cosa que pueda ocasionar daños a un equipo de cómputo.

Información Privada: Es aquella sobre la cual el titular posee un derecho exclusivo de uso o conocimiento pero que en mayor o menor medida es conocida por un grupo de personas a su alrededor y por el estado respondiendo a fines de garantía de los derechos del ciudadano.

Información íntima: Es aquella sobre la cual el titular tiene la absoluta exclusividad de su conocimiento y divulgación, que se encuentra ligada a sus procesos internos de selección y no puede ser conocida ni aun en circunstancias especiales por persona alguna ni por el estado.

Crimen cibernético: es cualquier acto criminal que se realice a través de una computadora.

Hacker: es una persona que goza, alcanzando un conocimiento profundo sobre el funcionamiento interno de un sistema, de una computadora o de una red de computadoras.

Cracker: Es una persona que intenta acceder a un sistema informático con malas intenciones, sin autorización.