UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES

CAMPUS ARAGON

LA INFORMÁTICA Y SUS REPERCUSIONES JURÍDICAS EN EL DERECHO PENAL MEXICANO

T E S I S

QUE PARA OBTENER EL TÍTULO DE
LICENCIADO EN DERECHO
P R E S E N T A:

GONZÁLEZ ESCOBAR ERNESTO

ASESOR

SEDEÑO CEA VELIA

SAN JUAN DE ARAGON ESTADO DE MÉXICO DEL 2003

AGRADECIMIENTOS DEDICADOS A:

A DIOS

GRACIAS POR PERMITIRME VIVIR Y GOZAR MI CAMINO Y ASI HABER PODIDO REALIZAR UNO DE MIS MAS GRANDES ESFUERZO EL SER PROFESIONISTA.

A MIS PADRES

A MI PADRE EL LIC. ERNESTO GONZALEZ HERNANDEZ POR BRINDARME TODO SU APOYO Y COMPRENSION Y ASÍ HABER PODIDO ALCANZAR UNO DE MIS MAS GRANDES ANHELOS EL SER PROFESIONISTA. Y ASI COMO TAMBIEN A MI MADRE LA SRA. GRACIELA ESCOBAR JAUREGUI QUIEN GRACIAS A SU AYUDA COMPRENSION Y PACIENCIA HA HECHO MAS LIGERO MI CAMINO PARA ENFRENTAR LA VIDA Y ASÍ HABER PODIDO LOGRAR MI META.

A MIS HERMANOS

A MI HERMANA LA CD JOCELYN GONZALEZ ESCOBAR Y A MI HERMANO EL LIC. OSCAR XAVIER GONZALEZ ESCOBAR. QUIEN GRACIAS A SU APOYO DEPOSITARON EN MI UNA GRAN CONFIANZA PARA LO CUAL FUE Y ES MUY NECESARIA PARA HABER PODIDO TERMINAR MIS ESTUDIOS PROFESIONALES POR LO CUAL ME SIENTO MUY ORGULLOSO DE ELLO.

A MI ASESORA

A LA LIC. VELIA SEDEÑO CEA POR HABERME BRINDADO SUS CONOCIMIENTOS Y TIEMPO DURANTE EL TRANSCURSO DE LA INVESTIGACION Y ASI HABER PODIDO LOGRAR DE ESTE TRABAJO UN VERDADERO EXITO.

A LA UNAM (ENEP ARAGÓN)

POR QUE GRACIAS A LA UNIVERSIDAD QUE ME ABRIO SUS PUERTAS Y DARME LA OPORTUNIDAD DE REALIZAR UNA CARRERA EN LA ENEP ARAGON Y ASI HABERME PODIDO SENTIR MUY CONTENTO Y SATISFECHO DE MIS EXITOS DURANTE MI ESTANCIA EN ELLA Y HOY PODER DECIR ORGULLOSAMENTE QUE SOY UNIVERSITARIO.

POR TODO Y POR MUCHO MAS....

GRACIAS

D

ÍNDICE GENERAL

INTRODUCCIÓN

Mucho se habla de los beneficios que los medios de comunicación y el uso de la Informática han aportado a la sociedad actual, pero el objetivo de mi trabajo será analizar la otra cara de la moneda, o sea, las conductas delictivas que puede generar el gran avance tecnológico, sobre todo en el campo de la informática.

El desarrollo tan amplio de las tecnologías informáticas ofrece un aspecto negativo: ha abierto la puerta a conductas antisociales y delictivas que se manifiestan de formas que hasta ahora no era posible imaginar. Los sistemas de computadoras ofrecen oportunidades nuevas y sumamente complicadas de infringir la ley, y han creado la posibilidad de cometer delitos de tipo tradicional en formas no tradicionales.

No es de extrañar que al preparar esta introducción, desde la tranquilidad de un hogar, se este entrelazado por medio de la tecnología digital con información proveniente desde los puntos más lejanos del mundo, o tener el acceso a nuestras cuentas corrientes, o simplemente encontrarnos leyendo las noticias nacionales e internacionales, sin necesidad de recurrir al diario de papel o estar en contacto con nuestros familiares en todo momento, ubicación y situación posible. Todos estos alcances en la comunicación se han ido posicionando en nuestras vidas, lo que para nosotros es nuevo y novedoso, futuras generaciones recordaran estos tiempos como el comienzo de una nueva era, la era digital y de la globalización de las comunicaciones.

En los últimos tiempos, ha sido evidente que la sociedad ha utilizado de manera benéfica los avances derivados de la tecnología en diversas actividades; sin embargo, es necesario que se atiendan y regulen las cada vez más frecuentes consecuencias del uso indebido de las computadoras y los sistemas informáticos en general.

Los llamados delitos informáticos no son cometidos por la computadora, sino que es el hombre quien los comete con ayuda de aquella. En ese entendido, mi trabajo se dirige al análisis de las posibles medidas preventivas, ya sean de carácter administrativo o penal que considero deben ser tomadas en cuenta para evitar que la comisión de este tipo de infracciones o delitos, no alcance en México los niveles de peligrosidad que se han dado en otros países.

Estas nuevas herramientas son usadas por personas, que por naturaleza humana nos hace enfrentar situaciones que se alejan de un claro comportamiento de convivencia en sociedad, en que con sus acciones utilizan para si y en desmedro de otros nuevas técnicas de criminalidad para el cometido de sus acciones perturbadoras. Estas acciones perturbadoras de la convivencia social han nacido al amparo de las nuevas herramientas tecnológicas, ante lo cual en el ámbito mundial, se ha generado una percepción de la seguridad informática, percepción que se ha ido desarrollando muy por detrás de la realidad de los alcances de los llamados ciberdelitos, pero que ha generado acciones claras y evidentes de una necesidad de control por parte de los organismos de control social formal; es por ello que las experiencias desarrolladas por la Organización de las Naciones Unidas, la Comunidad Europea, los Estados Unidos de Norteamérica, se han dirigido hacia la creación de los organismos necesarios para plantear que el problema del cibercrimen y sus consecuencias en la seguridad de las personas y

en sus respectivas economías es un hecho grave y que requiere de urgentes medidas para prevenirlo, tanto en el ámbito legislativo, de tecnologías y de socialización.

Al iniciar mi trabajo, encontré que no existe un concepto en cuanto al concepto de delito informático, y que estudiosos del tema lo han definido desde diferentes puntos de vista como son formal, típico y atípico, etcétera; dando lugar a que la denominación de esta conducta haya sufrido diferentes interpretaciones, las que recogí en la primera parte de este trabajo. Además señale los sujetos, activos y pasivos, clasificación y los tipos de delitos informáticos considerados tanto en la doctrina como en la legislación de diferentes países.

Seguidamente, analizare un estudio comparativo de la problemática de los delitos informáticos en los países tanto de Europa como de América, donde mayor incidencia ha tenido este fenómeno, el tratamiento penal que algunos gobiernos le han dado, y la parcial inercia que otros han mantenido sobre el tema, lo que se ha traducido en proyectos que hasta el momento no han fructificado.

A continuación, analice la regulación que han tenido en la legislación mexicana las conductas ilícitas relacionadas con la informática. Para ello estudie los antecedentes que a nuestro juicio han tenidos las regulaciones vigentes en esta materia como El Tratado de Libre Comercio de América del Norte.

Para finalizar el presente trabajo, determine algunas consideraciones sustentadas en el estudio comparativo antes mencionado, que trata de adecuar a la realidad existente en México, pero previendo que no estamos exentos de la velocidad del desarrollo tecnológico y de las exageraciones que éste genera.

En este trabajo enfoque mi atención en el derecho a la información, como bien jurídico que resulta afectado con los delitos informáticos. A partir de allí, analizare las conductas ilícitas que lo afectan y la forma como el citado derecho no es protegido por la legislación mexicana por supuesto de carácter penal..

El propósitos con este trabajo son, de una parte, analizar el estado en el cual se encuentra nuestra legislación mexicana respecto a la protección del derecho a la información; y otra parte, realizar aportes que sean útiles para la creación y aplicación de las normas jurídico penales sobre la materia.

CAPITULO I

ANÁLISIS Y OBJETIVOS DEL PROBLEMA ASI COMO SUS ANTECEDENTES HISTORICOS GENERALES.

PAGINACION DISCONTINUA

1.1PLANTEAMIENTO DEL PROBLEMA

Nuestra era, se caracteriza por una creciente acceso a la tecnología y una globalización social de la información y de la economía. El desarrollo tecnológico y el mayor uso de redes abiertas, como el Internet en los próximos años, proporcionaran oportunidades nuevas e importantes y plantearan nuevos desafíos. La estructura de la información se ha convertido en una parte vital del eje de nuestra economía los usuarios no pueden confiar en la disponibilidad en los servicios informativos y tener la seguridad de que sus comunicaciones y sus datos están protegidos frente al acceso o a la modificación no autorizadas, el desarrollo del comercio electrónico y la realización completa de la sociedad de la información depende de ellos.

El uso de las nuevas tecnologías digitales y de la telefonía inalámbrica ya se ha generado. Estas tecnologías nos brinda la libertad para poder movernos y permanecer comunicados y conectados con miles de servicios construidos sobre redes de redes, nos da la oportunidad de participar de enseñar y aprender, de jugar y trabajar juntos, y de intervenir en el proceso político.

Además la sociedad depende cada vez mas de esta tecnología, será necesario utilizar medios jurídicos, y prácticos eficaces para prevenir los riesgos asociados, las tecnologías de la sociedad de la información puede utilizarse y se utilizan para perpetrar y facilitar diversas actividades delictivas. En manos de personas que actúan de mala Fe, con mala voluntad o con negligencia grave, esta tecnología puede convertirse en instrumentos para actividades que ponen en peligro o atenten contra la vida, la propiedad o la dignidad de los individuos o del interés público.

En el enfoque clásico de la seguridad existe una comparación organizativa, geográfica y estructural estricta de la información según su sensibilidad y su categoria, esto no es ya prácticamente posible en la practica en el mundo digital, puesto que el tratamiento de la información se distribuye, se prestan servicios a usuarios móviles, y la interoperabilidad de los sistemas de una condición básica los enfoques tradicionales de la seguridad son sustituidas por soluciones.

Estas soluciones implica el uso del cifrado y las firmas digitales, de nuevos instrumentos de autenticación electrónica y de control del acceso, y de filtros de software de todo tipo, garantiza infraestructura de información segura y fiable no solo existe la aplicación de diversas tecnologías sino también su correcto despliegue y su uso efectivo.

Alguna de estas tecnologias existen ya, pero a menudo los usuarios no son concientes de su existencia de la manera de utilizarlas o de las razones de las que puedan ser necesario esta ultima circunstancia esta muy frecuente arraigado en la cultura nacional, de no enfrentar esta situación con la debida anticipación negándonos, la oportunidad de tener una clara percepción sobre esta grave problemática.

1.2 RELEVANCIA DEL PROBLEMA

La delincuencia informática se comete en el ciberespacio y no se detiene en las fronteras nacionales convencionales, en principio puede perpetrar desde cualquier lugar y contra cualquier usuario del mundo.

Se necesita una acción eficaz, tanto en el ámbito nacional como internacional, para luchar contra la delincuencia informática, a escala nacional, no hay respuestas globales y convocación internacional frente a los nuevos retos de la seguridad de la red y de la delincuencia informática en los países que enfrentan el problema así como las reacciones frente a la delincuencia informática se centran en el desarrollo nacional descuidando medidas alternativas de prevención . A pesar de los esfuerzos de la organización internacional y supranacional, las diversas leyes nacionales y de todo el mundo ponen de manifiesto considerables diferencias, especialmente de las disposiciones del derecho penal sobre piratería informática, protección del secreto comercial y contenidos ilícitos. También existen considerables diferencias en cuanto al poder coercitivo, de los organismos investigadores (especialmente por lo que respecta a los datos cifrados y a la investigación de redes internacionales), la jurisdicción en materia penal, y con respecto a la responsabilidad de los proveedores de servicios intermediarios para una parte y los proveedores de contenidos por otro.

A escala internacional y supranacional se ha reconocido ampliamente la necesidad de la lucha eficazmente contra la delincuencia informática y las diversas organizaciones han coordinado e intentado armonizar actitudes al respecto.

Todas estas acciones internacionales no han logrado calar en nuestra realidad y lograr cambiar la nula percepción de seguridad que sentimos a estos nuevos hechos, cabe destacar la reciente creación de parte de la policía de investigaciones de la brigada del cibercrimen, creada en los EEUU y que tienen equipos de especialistas dedicados a la localización de *hackers*, frente a sabotajes e intervención en caso de siniestros informáticos. Por otra parte, algunas policías

como el *FBI Y SCOTLAND YARD* disponen de unidades especiales para investigar la comisión de delito. pero no tiene como fundamento la de perseguir y llevar ante los tribunales de justicia a los hechos de este tipo de acciones que anualmente pueden causar daño económicos.

1.3 OBJETIVOS GENERALES

Dar un acercamiento sobre la realidad que acontece en México sobre la problemática que afecta nuestra sociedad y que tiene relación sobre el uso de la informática computacional como medio o fin para la comisión de delitos.

Otorgar los elementos de información necesarios para lograr una percepción social conveniente a fin de poder desarrollar una política de seguridad en México.

Dar una propuesta real de acción para México con el fin que sus recursos humanos y materiales se aboquen al estudio, análisis y evaluación de esta problemática delincuente desarrollando los cursos necesarios para poder ser sorprendidos y sobre pasados por esta nueva realidad nacional e internacional.

1.4 OBJETIVOS ESPECÍFICOS

Realizar una síntesis de la fortaleza y disponibilidad que presenta México para enfrentar la problemática de los delitos informaticos.

Realizar en el plano externo de la sociedad mexicana las oportunidades y amenazas a que se ve enfrentado México para enfrentar la problemática de los delitos informaticos.

Determinada sobre las bases de las legislaciones comparada la trascendencia que ha adoptado el tema de los delitos informaticos en otra área geográfica del mundo.

La propuesta conveniente para que México asuma responsabilidad como ente cooperador de la justicia y elementos fundamental en el control social formal y acepte el desafió de ingreso a un nuevo campo de estudio y acción de esta nueva topologia de delincuencia emergente.

México debe de enfrentar la globalización de la información económica y social. Como medio, deben ponerse a la vanguardia en México como en el resto del mundo en el estudio, análisis y control de estos hechos que transgreden la realidad social.

Realizar una metodologia científico-técnico en el ámbito de la informática a fin de adoptar una labor policial preventiva, investigadora, acorde a esta nueva y muy singular área de trabajo.

Así como también:

- Conceptualizar la naturaleza de los Delitos Informáticos
- Estudiar las caracteristicas de este tipo de Delitos
- Tipificar los Delitos de acuerdo a sus caracteristicas principales
- Investigar el impacto de éstos actos en la vida social y tecnológica de la sociedad
- Analizar las consideraciones oportunas en el tratamiento de los Delitos Informáticos

- Mencionar las empresas que operan con mayor riesgo de ser víctimas de ésta clase de actos
- Analizar la Legislatura que enmarca a ésta clase de Delitos, desde un contexto Nacional e Internacional.
- Definir el rol del auditor ante los Delitos Informáticos
- Presentar los indicadores estadísticos referentes a éstos actos delictivos

1.5 ALCANCES Y LIMITACIONES

ALCANCES

Esta investigación sólo tomará en cuenta el estudio y análisis de la información referente al problema del Delito Informático, tomando en consideración aquellos elementos que aporten criterios con los cuales se puedan realizar juicios valorativos respecto al papel que juega la Auditoria Informática ante éste tipo de hechos.

LIMITACIONES

La principal limitante para realizar ésta investigación es la débil infraestructura legal que posee nuestro país con respecto a la identificación y ataque a éste tipo de Delitos, no obstante se poseen los criterios suficientes sobre la base de la experiencia de otras naciones para el adecuado análisis e interpretación de éste tipo de actos delictivos.

1.6 ORIGEN DEL INTERNET

En Internet surgió primero el correo electrónico, como medio de comunicación entre las personas, los científicos y académicos quienes encontraron dentro de

este medio un instrumento para discutir e intercambiar resultados y avances de investigaciones. Estas fuerón las primeras comunidades virtuales.

Luego surgieron otros servicios de comunicación entre computadoras que facilitaron el auge de las comunidades virtuales. Por una parte, tenemos los *Newsgroups* de USENET y las listas o conferencias electrónicas que son instrumentos de comunicación en tiempo diferido y por la otra, ambientes de comunicación en tiempo real, como el *chat*.

Después de esta etapa, los internautas descubrieron que Internet podía servir de plataforma para crear una gigantesca biblioteca electrónica, donde se podían almacenar enormes cantidades de información. Así surgió el *Gopher* y casi inmediatamente después el *World Wide Web*.

Actualmente, se está produciendo una convergencia entre servicios de almacenamiento y búsqueda de información y servicios de comunicación. El *Web* permite integrar funciones de comunicación y así ha dado nacimiento a las comunidades virtuales que poseen un sitio web como centro de coordinación tanto de reservados de información como de comunicaciones. El sitio *web* se ha convertido en el territorio de la comunidad virtual, en un territorio "electrónico".

"*The Well*" fué la primera comunidad virtual, creada en 1985 por un grupo de ecologistas vinculados a empresas tecnológicas. Según sus propias palabras es "literalmente un pozo de agua para pensadores con diferentes tipos de vida, sean ellos artistas, periodistas, programadores, educadores o activistas". Los miles de miembros de "*Well*" se conectan casi a diario para participar en conferencias de temas tan amplios como arte, negocios o computadores, todo después de firmar

un compromiso de derechos y responsabilidades, con libertad de expresión, pero obligando a cada uno de sus asiduos visitantes a responsabilizarse de sus palabras.([1])

La Agencia de Proyectos de Investigación Avanzada (ARPA) se inicio en el departamento de defensa de los Estados Unidos en los últimos años de la década de los cuarenta para investigar los campos y tecnologia militar. El objetivo de la propuesta era plantear una red que tuviera la máxima resistencia ante cualquier ataque enemigo. Se suponia que una red de comunicaciones, por si misma, no es fiable debido a que parte de ella podria ser destruida durante un ataque Bélico.

Por lo tanto cada uno deberia mantener la misma importancia que los demás para garantizar que no pudiera ser un punto critico que pudiera dejar la red inactiva o fuera de servicio.

En 1968 el laboratorio fisico nacional en Inglaterra estableció la primera red de prueba basada en estos principios. En el mismo año, el primer diseño basado en estos principios de envió de paquetes de información realizado por Lawrence. Roberto, fué presentado en la ARPA. La red se llamo ARPANET.

[1]TONIATTI. Roberto. "Libertad informática y derecho a la protección de los datos personales: principios de legislación comparada". Revista Vasca de Administración Pública. No. 29. Enero-Abril. 1991. España. p.139 -162.

Al año siguiente el departamento de defensa dio en el envió bueno para comenzar la investigación en ARPANET. El primer nodo, fué la Universidad de California en los Ángeles pronto le siguieron otros tres nodos, la Universidad de California en Santa Bárbara, el instituto de investigación de Stanford y la Universidad de UTA. Estos sitios (como denominamos a los nodos) constituyeron la red original de cuatro nodos de ARPANET. Los cuatro nodos podría transferir datos en ellos en líneas de alta velocidad para compartir recursos informaticos.

El comienzo de la década de los setenta vio el crecimiento de la popularidad del correo electrónico sobre redes de almacenamiento y envió. En 1971, ARPANET había crecido hasta 15 nodos en 23 ordenadores *hosts* comienzan a utilizar un protocolo de control de redes, pero todavía falta una estandarización. Además había diferentes tipos de *hosts* por lo que el progreso en desarrollo los diferentes tipos de interfaces era muy lento.

En 1972 Larry Roberts de DARPA decidió que el proyecto necesitaba un empujón. Organizo la presentación de ARPANET en la conferencia internacional para investigar sobre los protocolos de comunicación que permitieran a ordenadores conectados a la red, comunicarse de una manera transparente a través de la transmisión de paquetes de información.

También en 1972 *Bolt, Beranek, Newman* (BBN) produjeron una aplicación de correo electrónico que funcionaba en redes distribuidas como ARPANET. El programa fué un gran éxito que permitió a los investigadores coordinarse y colaborar en sus proyectos de investigación y desarrollar las comunicaciones personales. Las primeras conexiones internacionales se establecieron en la universidad *College London*, en Inglaterra y en el *Royal Radar Establishment*, en

Noruega, junto con los ahora 37 nodos en EE.UU la exposición era muy fácil debido a esa estructura descentralizada.

En 1974 se estableció el Transmisión control protocolo (TCP) creado por Vinton Cerf y Bod que luego fué desarrollado hasta convertirse en el Transmisión control protocolo/ Internet convirtiendo los mensajes en pequeños paquetes de información que viajan por la red de forma separada hasta llegar a su destino donde vuelven a reagruparse.

IP maneja el direccionamiento de los envios de datos asegurando que los paquetes de información separados se encaminen por vias separadas a través de diversos datos, a través de múltiples redes con arquitectura distinta.

En julio de 1975 ARPANET fué transferido por DARPA a la agencia de comunicación de defensa de los diferentes países Europeos.

El crecimiento de ARPANET hizo necesario algunos órganos de gestión. El Internet *Configuration Control Boord* fué formado por ARPA en 1979 más tarde se transformó en el Internet *Activities Board* y en la actualidad es el Internet *Architecture Board of the internet societ.*

ARPANET en si mismo permaneció estrechamente controlado por el DOD hasta 1983 cuando su parte estrictamente militar que posteriormente se convirtió en *Milnet*. La *European Unis Network (EuNet)*, conectado a ARPANET se creó en 1982 para proporcionar su vicio de correo electrónico y servicios *Usenet*, a diversas organizaciones usuarios en los países bajos Dinamarca, Suecia e Inglaterra.

En 1984 el numero de servicios conectados a la red habia ya superado los 1,000 datos que en el Software de TCP/IP era de dominio público y la tecnología básica en el Internet (como ya se denomina esta red internacional expedida) era algo anárquica debido a su naturaleza, era difícil evitar que cualquier persona de disposición del necesario hardware (normalmente en universidades o gran empresas tecnológicas) se conoce a la red desde múltiples sitios.

En 1986 la *National Science Foundatio* (Fundación Nacional de Ciencias) de EE.UU inicio el desarrollo de NSTNET que se diseño originalmente para conectar cinco superordenadores. Su interconexión con el Internet requeria unas líneas de muy alta velocidad esto incremento el desarrollo tecnológico de INTERNET y brinda a los usuarios mejor infraestructura de las telecomunicaciones, otras agencias de administración norteamericanas entraron en Internet con sus inmensos recursos informaticos y comunicaciones NASA y el departamento de energía.

El día 1 de noviembre de 1988 Internet fué "infectado" con un virus de tipo "gusano", hasta el 10% de todos los servicios conectados fueron afectados el consentimiento subrayó la falta de adecuados mecanismos de seguridad en Internet por lo cual DARPA formó el *Computer Emergency Reponse Team* un equipo de reacción rápida que mantiene datos sobre todas las incidencias en red y sobre las principales amenazas.

En 1989 el número de servicios conectados a Internet alcanza a los 100.000 en ese mismo año se inaugura la primera conexión de un sistema de correo electrónico comercial a Internet, una nueva época a punto de empezar, la de la explotación.

ARPANET como entidad se extinguió en 1989 habiendo superado con mucho los objetivos y metas que tenía en su origen, los usuarios de la red apenas lo notaron ya que sus funciones no solamente continuaron sino que manejan notablemente a través de nuevos órganos mas representativos de la utilización actual en la red.

En 1990 redes de diversos países como España, Argentina , Australia, Brasil, Chile, Irlanda, se conectaron también a NSTNET.

En 1991 se retiran las restricciones de NFS a los usos comerciales INTERNET ese mismo año también se conectaron mas paises a la NSFNET , Croacia, Hong Kong, República Checa, Hungria, Polonia y Túnez.

En 1992 el número de servidores conectados a Internet sobrepasa la cifra de un millón de servidores. En ese año la sociedad de Internet se informo para proporcionar el intercambio global de información. *La Internet Architecture Boord*, fué reorganizada para llegar a formar parte de ISOC.

Como acontecimiento clave en la historia reciente en la historia del Internet, también en 1992 se desarrollo *World Wide Welo* en el laboratorio Europeo de fisica en Suiza, Esta tecnología provocó un drástico cambio en la apariencia, en el sentido y en el uso de Internet.

En 1993 el número de servidores Internet superaba los 2.000.000 también NST proporciona la información de una nueva organización INTERNIC, creada para proporcionar servicios de registro en Internet y base de datos en dirección. El

conocido navegador WWW *"Mosaic"* se desarrollo en el nacional *Center for super computing* en Europa.([2])

El número de servidores en Internet alcanza a los 3.800.000 en 1994, las primeras tiendas de Internet empieza aparecer junto con emisores de radio on-line.

En 1995 había mas de 5 millones de servidores conectados a Internet la espina dorsal en NSFNET empieza a ser sustituido por proveedores comerciales interconectados.

1.7 ANTECEDENTES GENERALES DEL DELITO INFORMATICO

Un análisis de las legislaciones que se han promulgado en diversos 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.

Desde hace aproximadamente diez años la mayoría de los países europeos han hecho todo lo posible para incluir dentro de la ley, la conducta punible penalmente, como el acceso ilegal a sistemas de computo o el mantenimiento ilegal de tales accesos, la difusión de virus o la interceptación de mensajes informáticos.

---

[2] COMISION DE LAS COMUNIDADES EUROPEAS. Comunicacion de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones. Contenidos ilícitos y nocivos en Internet. Bruselas. 16.10.1996 COM (96) 487 final.

En la mayoria de las naciones occidentales existen normas similares a los paises europeos. Todos estos enfoques están inspirados por la misma preocupación de contar con comunicaciones electrónicas, transacciones e intercambios tan confiables y seguros como sea posible.

Dar un concepto sobre delitos informáticos no es una labor fácil y esto en razón de que su misma denominación alude a una situación muy especial, ya que para hablar de "delitos" en el sentido de acciones tipificadas o contempladas en textos jurídico-penales, se requiere que la expresión "delitos informáticos" este consignada en los códigos penales, lo cual en nuestro país, al igual que en muchos otros, no ha sido objeto de tipificación aún; sin embargo, muchos especialistas en derecho informático emplean esta alusión a los efectos de una mejor conceptualización.

De esta manera, el autor mexicano **JULIO TÉLLEZ VALDÉS** señala que los delitos informáticos son "actitudes ilícitas en que se tienen a las computadoras como instrumento o fin (concepto atípico) o las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin (concepto típico)" en el sentido que las computadoras sólo es un instrumento que sirve para lograr sus objetivos y así poder penetrarse en las redes cibernéticas. Por su parte, el tratadista penal italiano **CARLOS SARZANA**, sostiene que los delitos informáticos son "cualquier comportamiento criminal en que la computadora está involucrada como material, objeto o mero símbolo".([3])

3 SARZANA, Carlo. "Criminalita e tecnologia" en Computers Crime. Rassagna Penitenciaria e Criminologia. Nos. 1-2. Ano 1. 1979. Roma. Italia. P.53

A raíz de la gran trascendencia que ha adquirido la informática, algunos autores como R. Hartley, aseveran que esta puede ser medidas en función de su utilidad, así la cantidad de información será proporcionada al numero de alternativas que se dispongan en un momento dado.([4])

Según **TÉLLEZ VALDÉS**, este tipo de acciones presentan las siguientes características principales:

a. Son conductas criminales de cuello blanco (*white collar crime*), en tanto que sólo un determinado número de personas con ciertos conocimientos (en este caso técnicos) pueden llegar a cometerlas.
b. Son acciones ocupacionales, en cuanto a que muchas veces se realizan cuando el sujeto se halla trabajando.
c. Son acciones de oportunidad, ya que se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico.
d. Provocan serias pérdidas económicas, ya que casi siempre producen "beneficios" de más de cinco cifras a aquellos que las realizan.
e. Ofrecen posibilidades de tiempo y espacio, ya que en milésimas de segundo y sin una necesaria presencia física pueden llegar a consumarse.
f. Son muchos los casos y pocas las denuncias, y todo ello debido a la misma falta de regulación por parte del Derecho.
g. Son muy sofisticados y relativamente frecuentes en el ámbito militar.
h. Presentan grandes dificultades para su comprobación, esto por su mismo carácter técnico.

[4] TELLEZ, Valdez Julio. Derecho Informatico. 2ª. ed. México. Ed. Mc Graw Hill 1996. p. 66

i. En su mayoría son imprudenciales y no necesariamente se cometen con intención.
j. Ofrecen facilidades para su comisión a los menores de edad.
k. Tienden a proliferar cada vez más, por lo que requieren una urgente regulación.
l. Por el momento siguen siendo ilícitos impunes de manera manifiesta ante la ley.

Asimismo, este autor clasifica a estos delitos, de acuerdo a dos criterios:

I. Como instrumento o medio.

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

a. Falsificación de documentos vía computarizada (tarjetas de crédito, cheques, etc.)
b. Variación de los activos y pasivos en la situación contable de las empresas.
c. Planeamiento y simulación de delitos convencionales (robo, homicidio, fraude, etc.)
d. Lectura, sustracción o copiado de información confidencial.
e. Modificación de datos tanto en la entrada como en la salida.
f. Aprovechamiento indebido o violación de un código para penetrar a un sistema introduciendo instrucciones inapropiadas.
g. Variación en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta bancaria apócrifa.
h. Uso no autorizado de programas de cómputo.

i. Alteración en el funcionamiento de los sistemas, a través de los virus informáticos.
j. Obtención de información residual impresa en papel luego de la ejecución de trabajos.
k. Acceso a áreas informatizadas en forma no autorizada.
l. Intervención en las líneas de comunicación de datos o teleproceso.

II. Como fin u objetivo.

En esta categoría, se enmarcan las conductas criminales que van dirigidas contra las computadoras, accesorios o programas como entidad física, como por ejemplo:

a. Programación de instrucciones que producen un bloqueo total al sistema.
b. Destrucción de programas por cualquier método.
c. Daño a la memoria.
d. Atentado físico contra la máquina o sus accesorios.
e. Sabotaje político o terrorismo en que se destruya o surja un apoderamiento de los centros neurálgicos computarizados.
f. Secuestro de soportes magnéticos entre los que figure información valiosa con fines de chantaje (pago de rescate, etc.).

Por otra parte, existen diversos tipos de delito que pueden ser cometidos y que se encuentran ligados directamente a acciones efectuadas contra los propios sistemas como son:

- **Acceso no autorizado:** Uso ilegítimo de *passwords* y la entrada de un sistema informático sin la autorización del propietario.
- **Destrucción de datos:** Los daños causados en la red mediante la introducción de virus, bombas lógicas, etc.
- **Infracción al copyright de bases de datos:** Uso no autorizado de información almacenada en una base de datos.
- **Interceptación de e-mail:** : Lectura de un mensaje electrónico ajeno.
- **Estafas electrónicas:** A través de compras realizadas haciendo uso de la red.
- **Transferencias de fondos:** Engaños en la realización de este tipo de transacciones.

Por otro lado, la red Internet permite dar soporte para la comisión de otro tipo de delitos:

- **Espionaje:** Acceso no autorizado a sistemas informáticos gubernamentales y de grandes empresas e interceptación de correos electrónicos.
- **Terrorismo:** Mensajes anónimos aprovechados por grupos terroristas para remitirse consignas y planes de actuación a nivel internacional.
- **Narcotráfico:** Transmisión de fórmulas para la fabricación de estupefacientes, para el blanqueo de dinero y para la coordinación de entregas y recogidas.

Otros delitos: Las mismas ventajas que encuentran en la Internet los narcotraficantes pueden ser aprovechadas para la planificación de otros delitos como el tráfico de armas, proselitismo de sectas, propaganda de grupos extremistas, y cualquier otro delito que pueda ser trasladado de la vida real al ciberespacio o al revés.

Los diferentes tipos de delitos cometidos por diferentes autores son muy diversos debido a que las personas que lo cometen tienen diferentes intenciones frente a los demás, en virtud de que algunos pueden ingresas a diferentes sistemas sin intención de perjudicas a alguien pero sin embargo lo hacen por lo cual ingresan sin conocimiento alguno.

Al respecto, según un estudio publicado en el Manual de las Naciones Unidas en la prevención y control de delitos informáticos (Nros. 43 y 44), el 90% de los delitos realizados mediante la computadora fuerón ejecutados por empleados de la propia empresa afectada. Asimismo, otro reciente estudio realizado en América del Norte y Europa indicó que el 73% de las intrusiones cometidas eran atribuibles a fuentes interiores y solo el 23% a la actividad delictiva externa.

Los esquemas básicos que utiliza un delincuente informatico es la aptitud a si como el reto que se proponen cada dia de mejorar sus conocimientos sobre la informática especialmente sobre las redes de Internet. Por tal motivo los delitos cometidos por estas personas no son considerados como tal debido a su amplio conocimiento que tienen, sin embargo se le considera como una persona respetable y no es considerado como un delincuente.

Las personas que cometen este tipo de delitos tienen caracteristicas especiales una de ellas que son personas que no se les puede complicar nada y todo lo pueden lograr por tal motivo se les considera como personas que no quieren cometer un delito simplemente quieren comprobar su capacidad.

Los estudiosos en este tipo de materias no están considerando a las personas que cometen este tipo de delitos como delincuentes debido que para que se les pueda

sancionar debe estar regulado en alguna legislación exclusivamente en el área penal, por tal motivo las personas que cometen este tipo de conductas solo puede quedar en la ética y en la conciencia de cada una de las personas que se dedican a la materia de la exploración de las redes y en consecuencia es muy difícil que se detengan a lograr sus objetivos ya que ellos mismos a veces no están conciente del daño que pueden causar a diferentes personas.([5])

De este modo se considera que los delitos llamados informaticos no puede tener una ligadura con los delitos cometidos habitualmente en virtud de que son muy diferentes sus características ya que los delitos convencionales son cometidos por todo tipo de personas y ya saben cual es el resultado de su sanción, mientras que los delitos informaticos no puede ser cometido por cualquier persona y por tal motivo conocen que al cometer cualquiera de estas faltas no pueden ser castigas por ninguna autoridad por que no se encuentra sancionado en alguna legislación por supuesto de carácter penal.([6])

1.8 ANTECEDENTES LEGALES

Los problemas jurídicos que se plantean a raiz de las actividades en el ciberespacio son de variada naturaleza, mucho de ellos previene del uso, de nombres identificatorios de los servidores que chocan con derechos de la propiedad industrial previamente adquiridos como la marca comercial registro de otros problemas provienen de la información que puede ser publicada en la red

[5] ROJAS PEREZ, Palacio Alfonso. Delito de Cuello Blanco. México. Ed Joaquín porrua 1986. p56
[6] ANIYAR DE CASTRO, Lolita. El Delito de cuello blanco en America Latina: una investigación necesaria. ILANUD AL DIA. Año 3 No. 8 Agosto 1980. San José. Costa Rica.

que puede afectar la honra de terceras personas derechos de propiedad intelectual (como el derecho de autor) o que puede importar la realización de actividades absolutamente prohibidas como la pornografía relativamente prohibida (como las apuestas) o frecuentemente protegidas (como la diseminación de datos privados) la existencia de legislaciones ordinarias independientemente de los países, la comisión de los delitos que no reconocen la existencia de las fronteras trasnacionales de los países y como lo menciona Carlos M. Correa como la "circulación a través de las fronteras internacionales de datos tratados por computadoras y/o medios magnéticos capturados vía satélite que puede ser consultados procesados o almacenados.([7]) Por ultimo existe toda la problemática que proviene del comercio electrónico realizado a través de estos medios tales como la formación del consentimiento la prueba de los contratos la legislación y la jurisdicción aplicable a dicha actividad las consecuencias fiscales etc.

1.9 ANTECEDENTES DE LA PROBLEMÁTICA NACIONAL

En México, el uso del Internet se remonta a finales de los años ochenta, siendo el primer país latinoamericano en conectarse a esta red en febrero de 1989, a través de los medios de acceso e interconexión de Teléfonos de México. Los primeros enlaces de Internet en el país fuerón hechos por el Instituto Tecnológico de Estudios Superiores de Monterrey, el Instituto Politécnico Nacional, la Universidad Nacional Autónoma de México, la Universidad de Guadalajara y la Universidad de las Américas en Puebla, con fines exclusivamente académicos. Desde entonces, el Internet y su uso, sobre todo a nivel internacional, carece de reglas formales, pero su uso se da en torno a consideraciones éticas, entre la

[7] CORREA M. . Carlos Derecho Informatico. Buenos Aires, Ed. Depalma. 1987. P 48

comunidad académica, originando una normativa no escrita, denominada "nettiquette". Es hasta 1994 en que se da inicio a la incorporación de instituciones comerciales en nuestro país, dando lugar a otra visión del fenómeno Internet.

No es de extrañar que al preparar este análisis, desde la tranquilidad de un hogar, se este entrelazado por medio de la tecnología digital con información proveniente desde los puntos mas lejanos del mundo, o tener el acceso a nuestras cuentas corrientes, o simplemente encontrarnos leyendo las noticias nacionales e internacionales, sin necesidad de recurrir al diario de papel o estar en contacto con nuestros familiares en todo momento, ubicación y situación posible. Todos estos alcances en la comunicación se han ido posicionando en nuestras vidas, lo que para nosotros es nuevo y novedoso, futuras generaciones recordaran estos tiempos como el comienzo de una nueva era, "la era digital y de la globalización de las comunicaciones".

El desarrollo de toda esta infraestructura en las comunicaciones, informaciones y negocios, que cada día más vemos compenetrados en las actividades políticas, culturales y comerciales de México, han mostrado un amplio crecimiento y desarrollo de todas las áreas del quehacer nacional, fenómeno mundial que ha ocasionando que el área dedicada a la informática y la computación ganan cada dia más un espacio. Las tecnologías de la sociedad de la información pueden utilizarse, y se utilizan, para perpetrar y facilitar diversas actividades delictivas. En manos de personas que actúan de mala fe, con mala voluntad, o con negligencia grave, estas tecnologías pueden convertirse en instrumentos para actividades que ponen en peligro o atentan contra la vida, la propiedad o la dignidad de los individuos o del interés público. Estas nuevas herramientas son usadas por personas, que por naturaleza humana nos hace enfrentar situaciones

que se alejan de un claro comportamiento de convivencia en sociedad, en que con sus acciones utilizan para sí y en desmedro de otros nuevas técnicas de criminalidad para el cometido de sus acciones perturbadoras. Estas acciones perturbadoras de la convivencia social han nacido al amparo de las nuevas herramientas tecnológicas, ante lo cual en el ámbito nacional, se ha generado una percepción de la seguridad informática, percepción que se ha ido desarrollando muy por detrás de la realidad de los alcances de los llamados ciberdelitos, pero que ha generado acciones claras y evidentes de una necesidad de control por parte de los organismos de control social formal.

Es por ello que las experiencias desarrolladas por la Organización de las Naciones Unidas, la Comunidad Europea, los Estados Unidos de Norteamérica, se han dirigido hacia la creación de los organismos necesarios para plantear que el problema del cibercrimen y sus consecuencias en la seguridad de las personas y en sus respectivas economías es un hecho grave y que requiere de urgentes medidas de todo tipo, tanto en el ámbito legislativo, de tecnologías y de socialización.

Esta situación de vulnerabilidad a que nos vemos enfrentados en el área de la protección legal de los derechos de las personas naturales o jurídica, no ha detenido el avance de otros medios, provenientes de la misma área tecnológica, para los resguardos de nuestros bienes jurídicos, tales como la privacidad, bienestar, derechos de autor y tantos otros; como son la aparición en el ámbito privado de servicios que mediante el uso de nuevas tecnologías o metodologías permiten un ambiente de tranquilidad relativa, especialmente en el desarrollo tecnológico nacional como internacional.

Como ya se dijo, aunque actualmente las computadoras se usan tanto en la fabricación de bienes como en la prestación de servicios, el elemento central más importante en cualquier sistema de computación es el factor humano. Es el hombre quien hace trabajar a éstas máquinas.

Su gran uso presente y que indudablemente se incrementará en el ejercicio y que permite predecir que las computadoras ejercerán un profundo efecto social, tanto en las personas como en las empresas. Dicho efecto se debe en gran parte a la cada vez mayor facilidad de comunicación entre el ser humano y la máquina, consecuencia de la evolución de los lenguajes de programación convirtiéndose en lenguajes corrientes o casi corrientes así como a la multitud de computadoras existentes en el mercado que cada vez son más potentes, más baratas y, por lo mismo, ya al alcance de un agente económico medio, lo que ha provocado una informática de masas que invade a toda la sociedad, quitándole así el carácter elitista que la investía en sus inicios.

Respecto al uso de las computadoras, Simon Nora y Alain Minc en su libro Informatización de la Sociedad, dicen:"Ayer las posibilidades de la informática estaban delimitadas; eran comerciales industriales o militares. De aquí en adelante, una infinidad de pequeñas máquinas y ocultarse ramificaciones ilimitadas de la informática."([8]).

La actual tecnología de computación anuncia innovaciones que modificará sustancialmente el curso de la civilización futura; se crearán herramientas y artefactos maravillosos: los cuales afectarán a los medios de comunicación, la

[8] NORA, Simon y MINC, Alain. La Informática de la sociedad, México. Fondo cultural Economia, 1981. p.50.

salud, la educación y las actividades de recreo, por mencionar algunas, pero también provocarán desórdenes, repercutiendo, sobre todo, en el empleo.

1.10 ANTECEDENTES DE LA PROBLEMÁTICA INTERNACIONAL

Durante milenios, el hombre fué cazador. La acumulación de innumerables actos de persecución de la presa le permitió aprender a reconstruir las formas y los movimientos de piezas de caza no visibles, por medio de huellas en el barro, ramas quebradas, estiércol, mechones de pelo, plumas, concentraciones de olores. Aprendió a olfatear, registrar, interpretar y clasificar rastros tan infinitesimales. Aprendió a efectuar complejas operaciones mentales con rapidez fulminea, en la espesura de un bosque o en un claro lleno de peligros.

"Generaciones y generaciones de cazadores fuerón enriqueciendo y transmitiendo todo ese patrimonio cognoscitivo. El cazador habria sido el primero en contar una historia, porque era el único que se hallaba en condiciones de leer, en los rastros mudos (cuando no imperceptibles) dejados por la presa, una serie coherente de acontecimientos"

En el párrafo anterior se evidencia que la información ha sido un factor fundamental en la existencia humana. El poder del hombre cazador surgia de su conocimiento de datos, y esa situación no se ha modificado a lo largo de la historia.

Los avances técnicos, científicos, médicos y sociales, fuerón posibles porque el ser humano registró sus experiencias en elementos materiales, que permitierón su

conocimiento por otros y las conservó para futura memoria. Ello se hizo, en principio, con medios tan rudimentarios como las pinturas rupestres y la escritura cuneiforme; luego con la imprenta; y ahora, con los sistemas electrónicos de información.

En el mundo moderno, el acceso a la información es un derecho que puede ejercerse libremente por cualquier persona, salvo cuando con él puedan afectarse otros como la intimidad, el patrimonio económico, la libre competencia o la seguridad..

"La tecnología de la información", como la denomina Vittorio Frosini , ha traído consigo una criminalidad a la cual la doctrina ha llamado genéricamente "delincuencia informática".

No obstante la ausencia de una legislación específica sobre la materia, el desarrollo doctrinal en relación con la delincuencia informática ha sido abundante ; la razón de ello, en nuestro criterio, es que la amplitud e importancia del tema permite su estudio desde distintas perspectivas y a partir de diferentes conductas ilícitas, cuyos modos de ejecución evolucionan al ritmo de la tecnología y del ingenio humano.

Nunca antes se había vivido una época como la actual con tanta velocidad de aplicación de los nuevos descubrimientos. Tal es el de la computadora, pues en un corto periodo ha habido reducciones sorprendentes en su tamaño y a medida en que ésta se ha reducido, también se ha decrecido el costo de su uso y ha aumentado su velocidad de operación, así como su capacidad de almacenamiento.

El empleo de la nueva tecnología es la causa de muchos de los cambios que ocurren: desde hace un siglo las transformaciones mas espectaculares tienen bases técnicas por lo que existe la facilidad de proyectar un futuro regido por la tecnología.

El creciente acceso a las computadoras personales que son mas baratas, mas pequeñas y mas poderosas, provocarán un importante cambio pues éstas no se encuentran aisladas como en sus inicios, sino unidas entre si en potentes redes.

Como las computadoras se utilizan tanto en la fabricación de bienes como en la prestación de servicios, desempeñan un preponderante papel económico. De ésta forma dichas maquinas están permitiendo, mediante la integración y disponibilidad de numerosos bancos de datos, la consecución de uno de los cometidos principales de la informática: La adecuada toma de decisiones.

Entre más sirva una información para reducir la incertidumbre en las decisiones efectuadas, mejor será su valor; sin embargo, como todo recurso básico, la información no es gratuita.

El costo de la información obtenida debe compararse con los beneficios conseguidos de su uso, por lo tanto, ésta debe ser exacta, oportuna, Completa y concisa, con lo que se mejora la calidad de las decisiones. si falta alguna de éstas características y que se explican a continuación, la calidad de las decisiones puede verse afectada:

a).EXACTITUD: Es el porcentaje de información correcta respecto al total de información generada en un periodo.

b).OPORTUNA: Se refiere a la puntualidad de la información, pues de nada sirve que ésta sea exacta si llega demasiado tarde para ser usada.

c).INTEGRIDAD: Es la reunión de los hechos disponibles que se encuentran diseminados con el objeto de proporcionar información más completa.

d).CONCISION: Es el resumen de los datos verdaderamente importantes para la toma decisiones.

Consideramos a la información como un recurso porque cuenta con los atributos de un recurso fisico:

1. Tiene valor como el dinero, las materias primas o la fuerza laboral.

2. Tiene caracteristicas que permiten su medición en términos de uso duración y efectos sobre otros recursos.

3. puede ser valorada en términos de recolección, almacenamiento y recuperación.

4. puede ser presupuestada y controlada.

5. puede valuarse en términos de costo y valor de uso con fines de administración.

Estos aspectos se puede explicar por la dificultad de reprimirla en forma internacional, ya que los usuarios están esparcidos por todo el mundo y, en consecuencia, existe una posibilidad muy grande de que cualquier sujetos este bajo leyes nacionales de los diferentes paises. Además, si bien los acuerdos de

cooperación internacional y los tratados de extradición bilaterales intentan remediar algunas de las dificultades ocasionadas por los delitos informáticos, sus posibilidades son limitadas. Sin embargo, a pesar de los perjuicios que acarrean las nuevas tecnologías, son más y mejores los beneficios que aportan por lo que estas acaban imponiéndose y dar por resultados cambios irrevocables, positivos o negativos, que es imposible detener. Nora y Minc dice al respecto: "Ninguna tecnología, por innovadora que sea, acarrea a la larga consecuencias fatales. Sus efectos son denominados por la evolución de la sociedad más de lo que la constriñen.([9])

Por su parte, Claude Shannon, menciona que a mayor y mejor información, menor será el desconocimiento de las personas.

De aquí se desprende, como dice el Dr. Julio Téllez Valdés, "que la información es un verdadero bien susceptible de apropiación con un innegable valor patrimonial inherente ([10])" por lo que la informática, dada su importancia económica, esté considerada como una parte medular en varios países que le conceden a su materia prima, la información, un verdadero valor. La información es poder.

La actual revolución informática, cuyo poder se funda en la computadora, está generando, entre otras cosas nuevos aumentos de productividad y cambios en la competencia, lo que provoca una intensa reorganización de la economía, la política, la cultura y desde el punto de vista social del mundo.

---

[9] Nora, Simon y MINC, Alain. Op. Cit. P.25
[10] TELLEZ. Valdés Julio. Op. Cit. P 68.

CAPITULO II

LA INFORMATICA EN EL CAMPO JURÍDICO

2.1 DEFINICIÓN DE DELITO

La noción del delito ha variado conforme a los momentos históricos, las áreas geográficas y la ideología de cada pueblo, de manera que es difícil establecer un concepto de honda raíz filosófica que tenga validez en cualquier momento y lugar; múltiples definiciones se han elaborado de acuerdo con diversas corrientes doctrinarias que han respondido a situaciones y necesidades específicas.([11])

Se ha definido el delito como *una acción punible.([12]) El código penal de 1931* lo define en su artículo 7º. *Como el acto u omisión que sanciona las leyes penales([13]). Así como acción u omisión como lo define el Artículo 15 del código penal reciente constitutivo de una infracción penal([14])*. Desde un punto de vista jurídico sustancial y en atención a sus elementos Jiménez de Asúa expresa que el delito es el:
Acto antijurídico, culpable, sometido a veces a condiciones objetivas de personalidad, imputable a un hombre y sometido a una sanción penal.([15])

Por lo tanto el doctor Jorge López Vergara expresa que son cuatro las grandes áreas que cubren el estudio del delito como es la conducta humana, la

[11] OSORIO Y NIETO. Cesar Augusto. Síntesis de Derecho Penal . Ed. Trillas. México 1984. p 43
[12] MEZGER. Edmundo. citado por Castellanos Tena Fernando. Lineamientos Elementales de derecho penal. Editorial Porua. México 1978 . pag 129.
[13] Código Penal para el Distrito Federal.
[14] DE PINA VARA. Rafael. Diccionario de Derecho. Ed. Porrua. México. 1996. p 219.
[15] JIMENEZ de Asúa. Luis. La Ley y el Delito. Editorial Hermes. Argentina. 1954. pag.223.

investigación de las causas de la delincuencia, la prevención del delito y el tratamiento del delincuente.([16])

Nosotros entendemos el delito, con base en la definición legal, como la conducta sancionada por las leyes penales expedidas con el objeto de proteger los bienes jurídicos fundamentales del individuo y de la sociedad.

2.2 QUE ES EL INTERNET

El Internet es uno de los fenómenos de mayor rápidez de penetración en la sociedad y en el mercado. Su impacto se está experimentando tanto en el ocio como en los negocios.

Los cambios fundamentales son cuatro:

- Como instrumento para informar e informarse
- Como nuevo canal de comunicación
- Como nuevo canal de formación y gestión del conocimiento
- Como herramienta de transacción comercial

La clave del éxito en Internet consiste en saber crear y mantener comunidades virtuales constituidas por personas que acuden a la comunidad para satisfacer sus expectativas o necesidades, para aportar su colaboración y para sentirse parte de

[16] LOPEZ VERGARA, Jorge. Introducción al estudio de la Criminología. Revista Mexicana de Derecho Penal. 5ª. Época, numero 4. Mexico 1978 p 43.

un colectivo del que recibe y al que aporta. Es decir, los contenidos son la razón que atrae a la gente, pero la sensación de comunidad es la que la retiene

El Internet es una red gigante que interconecta una innumerable cantidad de redes de computadoras locales, por lo que no es una entidad física o tangible. Es la red de las redes: pequeñas Redes de Área Local (LAN o Local Área *Network*), Redes de Área Metropolitana (MAN o Metropolitan Area *Network*) y grandes Redes de Área Amplia (*WAN o Wide* Área *Network*), que conectan a los sistemas informáticos de miles de organizaciones en el mundo. Se conectan a través de líneas telefónicas regulares hasta líneas de alta velocidad, fibra óptica, satélites y microondas.

Es imposible determinar su tamaño en un momento dado, aunque su crecimiento ha sido extraordinario en pocos años. En 1981, menos de 300 computadoras estaban conectadas al Internet; para 1989, eran menos de 90 mil computadoras. En 1993, aproximadamente un millón de computadoras estaban conectadas y, hoy en día, se calcula que son 9 millones 400 mil equipos huéspedes alrededor del mundo, de los cuales, aproximadamente 60% se encuentran localizados en los Estados Unidos. El diseño de la red en nuestro país se denomina multiprotocolo, debido a que su estructura está construida con diversos protocolos: TCP/IP, Novell, X.25, *Frame Relay*, ATM, SNA y protocolos de LAN. Los medios de transmisión son de diversas velocidades, dependiendo del que se utilice: satélite, microondas, cobre, fibra óptica, radio o celular.

El Internet como fenómeno se ha convertido en un tema polémico y contrastante, ya que puede ser usado como herramienta de acceso a información de contenido inmensamente valioso, con alcances enormes en el ámbito del arte, la cultura, la

ciencia y el desarrollo personal, o su abuso, dando lugar a fraudes, pornografía o corrupción de menores. Es un sistema internacional de intercambio de comunicación que une a personas, instituciones, compañías y gobiernos alrededor del mundo, de manera casi instantánea, pudiendo dirigirse a un individuo en específico o a un grupo amplio de personas interesadas en un tema, o al mundo en general.([17])

2.3 FUNCIONES DEL INTERNET EN LA SOCIEDAD

El Internet permite acceder a los siguientes servicios:

Acceso remoto a recursos de cómputo por interconexión. Es una herramienta interactiva que permite el acceso a programas y aplicaciones disponibles en otra computadora.

Comunicación en tiempo real. Cabe la posibilidad de transmitir mensajes en diálogos inmediatos o en tiempo real en Internet (*Internet Relay Chat o IRC*), permitiendo a dos o más personas escribir y que casi inmediatamente aparezca la comunicación en la pantalla del otro, sin importar la distancia geográfica. Esta forma de comunicación es análoga a la línea de teléfono, usando el teclado y el monitor, en lugar del auricular.

---

[17] MIR PUIG. S (Comp.) Delincuencia Informática. Promociones y Publicaciones Universitarias. Barcelona. 1992.

Correo electrónico. Es el servicio de mayor uso en cuanto a tráfico. Permite que se escriban y envíen mensajes a una persona o grupo de personas.

Grupos de discusión. Son personas unidas a través de la red en torno al estudio, análisis o discusión de un tema determinado. Existen hoy en día alrededor de quince mil grupos enfocados a diversos temas. En 1994, aproximadamente 70 mil mensajes diarios fueron enviados a diversos grupos de discusión y hoy en día, alrededor de 100 mil mensajes nuevos o artículos son enviados diariamente a grupos de discusión.

Transferencia de archivos remotos. Permite que los archivos se transfieran de una computadora a otra a distancia, pudiendo ser documentos, gráficas, hojas de cálculo, programas y sonido.

World Wide Web, a través del cual pueden ser transmitidos textos, gráficos, animaciones en forma de hipertexto, imágenes y sonido. El objetivo del WWW es servir de plataforma para almacenar, globalmente y en línea, conocimientos conteniendo información de diversas fuentes. Existen formatos estándares para que las páginas puedan ser publicadas, siendo ésta otra forma de normativa sin fronteras. Estos estándares son, a la vez, lo suficientemente flexibles y sofisticados, que permiten publicar las necesidades de grandes compañías, bancos, casas de cambio, periódicos y revistas que actualmente publican en línea ediciones de su material, así como oficinas gubernamentales, con el fin de diseminar información al público. Al mismo tiempo, la publicación de páginas es lo suficientemente simple que miles de personas que son usuarios independientes y organizaciones locales pequeñas usan el *Web* para publicar sus propias páginas, mismas que son accesibles a todo el mundo.

La libre expresión, la educación y el comercio tienen hoy en día en el Internet un medio interactivo invaluable a nivel mundial. Cualquier individuo puede tener acceso al ciberespacio en general y al Internet en particular usando una computadora personal que esté conectada directamente a una red que esté a su vez conectada al Internet, o puede usarse una computadora personal con un módem conectado a una línea telefónica que a su vez esté conectada a una computadora más grande o a una red que estén directa o indirectamente conectadas al Internet. Ambas formas de conexión son accesibles a las personas en una amplia variedad de entidades académicas, gubernamentales o a través de compañías proveedoras de acceso a Internet.

La "era de la información" impone en nuestro país, al igual que en el mundo globalizado, acciones concretas que deberían tender a la generalización de uso de la informática como herramienta de desarrollo social. Coincidimos con el concepto acerca de la importancia y sus contribuciones al desarrollo nacional, así como que "contribuye a fortalecer el ejercicio pleno de nuestra soberanía. A través de su empleo es posible realizar un seguimiento preciso y detallado de las características físicas del territorio. ofrece además, la posibilidad de ampliar y consolidar la presencia de México en el mundo y de reforzar la cultura e identidad nacionales al acrecentar las posibilidades de acceso a la información, permite una sociedad más consciente y con mayores oportunidades de participación en todas las actividades de la vida nacional. Ejercicio pleno de la soberanía, estado de derecho, desarrollo democrático, bienestar social y crecimiento económico son todos, objetivos nacionales en cuyo logro la evolución de la tecnología a influido en todos los tiempos y momentos y esto trae como resultado un gran paso a el futuro de nuevos aspectos de la vida cotidiana y así mismo se puede convertirse en un proceso para la nueva formación como la

informática puede contribuir de manera decisiva."([18]) Sin embargo, y aunque parezca contradictorio con las ideas expresadas en un principio, nos enfrentamos con el hecho de que la cultura de la informática y de la información en nuestro país es muy incipiente.

Lamentablemente el uso generalizado de la informática va de la mano con la realidad social y económica del país, con el nivel educativo de la población y, definitivamente, con la falta de cultura informática. En México, el uso de la computadora como instrumento o herramienta de trabajo, según datos del Instituto Nacional de Estadística, Geografía e Informática, es muy incipiente: en 1994 sólo existían 2.2 computadoras personales por cada 100 habitantes, ocupando nuestro país el número 28 a nivel mundial.

Lo anterior tiene una relación directa con el nivel de ingreso y se centraliza en poblaciones urbanas. De quienes tienen acceso a esta herramienta de trabajo (5.6% de la población urbana), el 29% la usa sólo en su trabajo. Los desarrollos actuales de interfaces gráficas intuitivas que hacen del Internet una herramienta informática simple de manejar carecen de sentido ante los indicadores estadísticos.

Las organizaciones sociales juegan un papel muy importante en la dinámica social contemporánea. El fomento de las comunidades de usuarios de redes mexicanas es esencial para el desarrollo del país, toda vez que propicia la unidad de grupos sociales de diversa naturaleza (género, indígenas, opinión, etc.). Es

---

[18] BIERCE, B. William. "El delito de violencia tecnológica en la legislación de nueva York" Derecho de la Alta Tecnología. Año 6 No. 66 Febrero 1994. Estados Unidos. P.20.

importante fomentar la creación de contenidos nacionales dada la carencia de fuentes de información en idioma español, con contenidos nacionales. México tiene la ventaja de poder aprender de las experiencias internacionales.

Definitivamente, la urgente reactivación económica salta a la vista, así como la necesidad de poner en práctica programas concretos de educación. El Instituto Latinoamericano de la Comunicación Educativa y la Secretaría de Educación Pública se encuentran ya en un proyecto piloto de integración de algunas escuelas primarias y secundarias de todos los Estados del país a la red de redes, con el fin de conformar una red informática educativa. Se pretende que en un futuro el Internet enlace al sistema educativo nacional a través de un sistema satelital. Se proyecta la creación de 300 centros de capacitación para maestros, que a su vez se conviertan en capacitadores. El proyecto, en el cual se dotará de un promedio de 5 computadoras por escuela, comprende 4 escuelas por Estado y 10 en el Distrito Federal.

2.4 LA INFORMATICA Y SU RELACIÓN CON EL DERECHO

El progreso cada día más importante y sostenido de los sistemas computacionales permite hoy procesar y poner a disposición de la sociedad una cantidad creciente de información de toda naturaleza, al alcance concreto de millones de interesados y de usuarios. Las más diversas esferas del conocimiento humano, en lo científico, en lo técnico, en lo profesional y en lo personal están siendo incorporados a sistemas informáticos que, en la práctica cotidiana, de hecho sin limitaciones, entrega con facilidad a quien lo desee un conjunto de datos que hasta hace unos años sólo podían ubicarse luego de largas búsquedas y

selecciones en que el hombre jugaba un papel determinante y las máquinas existentes tenían el rango de equipos auxiliares para imprimir los resultados. En la actualidad, en cambio, ese enorme caudal de conocimiento puede obtenerse, además, en segundos o minutos, transmitirse incluso documentalmente y llegar al receptor mediante sistemas sencillos de operar, confiables y capaces de responder casi toda la gama de interrogantes que se planteen a los archivos informáticos.

Puede sostenerse que hoy las perspectivas de la informática no tienen límites previsibles y que aumentan en forma que aún puede impresionar a muchos actores del proceso.

Este es el panorama de este nuevo fenómeno tecnológico-jurídico en las sociedades modernas. Por ello ha llegado a sostenerse que la Informática es hoy una forma de Poder Social. Las facultades que el fenómeno pone a disposición de Gobiernos y de particulares, con rapidez y el ahorro consiguiente de tiempo y energía, configuran un cuadro de realidades de aplicación y de posibilidades de juegos lícito e ilícito, en donde es necesario el derecho para regular los múltiples efectos de una situación, nueva y de tantas potencialidades en el medio social.([19])

Los progresos mundiales de las computadoras, el creciente aumento de las capacidades de almacenamiento y procesamiento, la miniaturización de los chips de las computadoras instalados en productos industriales, la fusión del proceso de la información con las nuevas tecnologías de comunicación, así como la

---

[19]ARTEGA S., Alberto. "El delito informático: algunas consideraciones jurídico penales" Revista de la Facultad de Ciencias Jurídicas y Políticas. No. 68 Año 33. Universidad Central de Venezuela. 1987. Caracas, Venezuela. P. 125-133.

investigación en el campo de la inteligencia artificial, ejemplifican el desarrollo actual definido a menudo como la era de la información.

Esta marcha de las aplicaciones de la informática no sólo tiene un lado ventajoso sino que plantea también problemas de significativa importancia para el funcionamiento y la seguridad de los sistemas informáticos en los negocios, la administración, la defensa y la sociedad.

Debido a esta vinculación, el aumento del nivel de los delitos relacionados con los sistemas informáticos registrados en la última década en los Estados Unidos, Europa Occidental, Australia y Japón, entre otros, representa una amenaza para la economía de un país y también para la sociedad en su conjunto.

De acuerdo con la definición elaborada por un grupo de expertos en mayo del 83, el término ***delitos relacionados con las computadoras*** se define como cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesado automático de datos y/o transmisiones de datos. La amplitud de este concepto es ventajosa, puesto que permite el uso de las mismas hipótesis de trabajo para toda clase de estudios penales, criminológicos, económicos, preventivos o legales.

En la actualidad la informatización se ha implantado en casi todos los países. Tanto en la organización y administración de empresas y administraciones públicas, particulares como en la investigación científica, en la producción industrial o en el estudio e incluso en el ocio, el uso de la informática es en ocasiones indispensable y hasta conveniente. Sin embargo, junto a las incuestionables ventajas que presenta comienzan a surgir algunas facetas

negativas, como por ejemplo, lo que ya se conoce como "criminalidad informática". ([20])

El espectacular desarrollo de la tecnología informática ha abierto las puertas a nuevas posibilidades de delincuencia antes impensables. La manipulación fraudulenta de los ordenadores con ánimo de lucro, la destrucción de programas o datos y el acceso y la utilización indebida de la información que puede afectar la esfera de la privacidad, son algunos de los procedimientos relacionados con el procesamiento electrónico de datos mediante los cuales es posible obtener grandes beneficios económicos o causar importantes daños materiales o morales. Pero no sólo la cuantía de los perjuicios así ocasionados es a menudo infinitamente superior a la que es usual en la delincuencia tradicional, sino que también son mucho más elevadas las posibilidades de que no lleguen a descubrirse. Se trata de una delincuencia de especialistas capaces muchas veces de borrar toda huella de los hechos.

En este sentido, la informática puede ser el objeto del ataque o el medio para cometer otros delitos. La informática reúne unas características que la convierten en un medio idóneo para la comisión de muy distintas modalidades delictivas, en especial de carácter patrimonial (estafas, apropiaciones indebidas, etc.). La idoneidad proviene, básicamente, de la gran cantidad de datos que se acumulan, con la consiguiente facilidad de acceso a ellos y la relativamente fácil manipulación de esos datos.

---

[20] AMOROSO Fernández, Yarina. "La informática como objeto de derecho." Algunas consideraciones acerca de la protección jurídica en Cuba de los Datos Automatizados" en Revista Cubana de Derecho. Unión Nacional de Juristas de Cuba. No. 1. Habana, Cuba. 1991. P.43.

El estudio de los distintos métodos de destrucción y/o violación del hardware y el software es necesario en orden a determinar cuál será la dirección que deberá seguir la protección jurídica de los sistemas informáticos, ya que sólo conociendo el mecanismo de estos métodos es posible encontrar las similitudes y diferencias que existen entre ellos. De este modo se pueden conocer los problemas que es necesario soslayar para conseguir una protección jurídica eficaz sin caer en el casuismo.

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

Si se tiene en cuenta que los sistemas informáticos, pueden entregar datos e informaciones sobre miles de personas, naturales y jurídicas, en aspectos tan fundamentales para el normal desarrollo y funcionamiento de diversas actividades como bancarias, provisionales y de identificación de las personas. Y si a ello se agrega que existen Bancos de Datos, empresas o entidades dedicadas a proporcionar, si se desea, cualquier información, sea de carácter personal o sobre materias de las más diversas disciplinas a un Estado o particulares; se comprenderá que están en juego o podrían ha llegar a estarlo de modo dramático, algunos valores colectivos y los consiguientes bienes jurídicos que el ordenamiento jurídico-institucional debe proteger.

No es la amenaza potencial de la computadora sobre el individuo lo que provoca desvelo, sino la utilización real por el hombre de los sistemas de información con fines de espionaje.

No son los grandes sistemas de información los que afectan la vida privada sino la manipulación o el consentimiento de ello, por parte de individuos poco conscientes e irresponsables de los datos que dichos sistemas contienen.

La humanidad no está frente al peligro de la informática sino frente a la posibilidad real de que individuos o grupos sin escrúpulos, con aspiraciones de obtener el poder que la información puede conferirles, la utilicen para satisfacer sus propios intereses, a expensas de las libertades individuales y en detrimento de las personas. Asimismo, la amenaza futura será directamente proporcional a los adelantos de las tecnologías informáticas.

La protección de los sistemas informáticos puede abordarse tanto desde una perspectiva penal como cualquier rama del derecho según sea el caso. Estas distintas medidas de protección no tienen porque ser excluyentes unas de otras, sino que, por el contrario, éstas deben estar estrechamente vinculadas. Por eso, dadas las características de esta problemática sólo a través de una protección global, desde los distintos sectores del ordenamiento jurídico, es posible alcanzar una cierta eficacia en la defensa de los ataques a los sistemas informáticos.

2.5 CONCEPTOS DE DELITOS INFORMATICOS

El *delito informático* implica actividades criminales que en un primer momento los países han tratado de encuadrar en figuras típicas de carácter tradicional, tales como robos, fraudes, falsificaciones, perjuicios, estafa, sabotaje, etcétera. Sin embargo, debe destacarse que el uso de las técnicas informáticas ha

creado nuevas posibilidades del uso indebido de las computadoras lo que ha propiciado a su vez la necesidad de regulación por parte del derecho.

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

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

Se hace necesario, presentar algunas definiciones elaboradas doctrinalmente, que han contribuido al esclarecimiento de lo que debe entenderse por delitos informáticos.

Para **Carlos Sarzana**, en su obra Criminalista e tecnología, los crímenes por computadora comprenden *"cualquier comportamiento criminogeno en el cual la computadora ha estado involucrada como material o como objeto de la acción criminógena, o como mero símbolo".*([21])

[21] Sarzana Carlos, citado por Téllez 1995 Op. Cit p.104

Nidia Callegari define al *delito informático* como *"aquel que se da con la ayuda de la informática o de técnicas anexas".*

Parker (citado por Cuervo, 1999) define los delitos informáticos como todo acto intencional asociado de una manera u otra a los ordenadores; en los cuales la victima ha, o habría podido sufrir una pérdida; y cuyo autor ha, o habría podido obtener un beneficio.([22])

Quiñónez (1997) define a los delitos informáticos como cualquier acto violatorio de la ley penal para cuya comisión exitosa es esencial el conocimiento y utilización de la tecnología de las computadoras.

Rafael Fernández Calvo define al *delito informático* como *"la realización de una acción que, reuniendo las caracteristicas que delimitan el concepto de delito, se ha llevado a cabo utilizando un elemento informático o telemático contra los derechos y libertades de los ciudadanos definidos en el titulo uno de* la *Constitución Española."([23])*

---

[22] GARVARINO, Alvaro, Curvelo, Carmelo, et all. "Nuevas normas jurídicas en materia informática" Revista de la Asociación de Escribanos del Uruguay. Vol. 76 No. 1 - 6. Enero-Junio 1999. Montevideo, Uruguay. P. 68-78.

[23] FERNANDEZ Calvo, Rafael. "El tratamiento del llamado delito informático" en el proyecto de ley Organico del Código Penal: reflexiones y propuestas de la CLI (Comisión de libertades e informática" en Informática y Derecho. P.1150.

Para **Tiedemann** (citado por Quiñones, 1997). Los delitos de informática serian cualesquiera que se realicen contra los bienes ligados al tratamiento automático de datos.

María de la Luz Lima dice que el *"delito electrónico " "en un sentido amplio es cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin y que, en un sentido estricto, el delito informático, es cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como método, medio o fin".(24)*

Julio Téllez Valdés conceptualiza al *delito informático* en forma típica y atípica, entendiendo por la primera a *" las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin"* y por las segundas *"actitudes ilícitas en que se tienen a las computadoras como instrumento o fin".(25)*

"**Zabale** y otros (2000) definen los delitos informáticos como toda conducta con cuyas características delictivas, es decir, sea típica, antijurídica y culpable y atente contra el soporte lógico de un sistema de procesamiento de información, y el cual se distingue de los delitos computacionales o tradicionales informatizados.

---

[24] LIMA DE LA LUZ, María. "Delitos Electrónicos" en Criminalia. México. Academia Mexicana de Ciencias Penales. Ed. Porrúa. . No. 1-6. Año L. Enero-Junio 1984. Pp.100.

[25] TELLEZ Valdés Julio . Op cit. P. 104

"En mi opinión particular defino a los delitos informáticos como: Aquellas conductas típicas, antijurídicas y culpables que lesionan la seguridad informática de los sistemas tecnológicos y dirigidas contra bienes intangibles como datos, programas, imágenes y voces almacenados electrónicamente".

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

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

Lógicamente este concepto no abarca las infracciones administrativas que constituyen la generalidad de las conductas ilícitas presentes en México debido a que la legislación se refiere a derecho de autor y propiedad intelectual sin embargo, deberá tenerse presente que la propuesta final de este trabajo tiene por objeto la regulación penal de aquellas actitudes antijurídicas que estimamos más graves como último recurso para evitar su impunidad.

Tales definiciones son suficientemente ilustrativas, por lo que tan sólo agregaríamos que la categoría denominada "delincuencia informática", como tema de estudio doctrinal, es útil para determinar el grado de conductas cometidas por medio de sistemas de procesamiento de datos, o en éstos, pueden lesionar bienes jurídicos vinculados a derechos individuales y así proceder a su

tipificación; y que permite al operador jurídico determinar cuándo se encuentra frente a una conducta antijurídica, por haber lesionado materialmente tales bienes jurídicos o haberlos puesto concretamente en peligro.

2.6 SUJETO ACTIVO DEL DELITO *"HACKERS"*

Las personas que cometen los *"Delitos Informáticos"* son aquellas que poseen ciertas características que no presentan el denominador común de los delincuentes, esto es, los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso de los sistemas informatizados, aún cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos.

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

El nivel típico de aptitudes del delincuente informático es tema de controversia ya que para algunos el nivel de aptitudes no es indicador de delincuencia informática en tanto que otros aducen que los posibles delincuentes informáticos son personas listas, decididas, motivadas y dispuestas a aceptar un reto tecnológico, características que pudieran encontrarse en un empleado del sector de procesamiento de datos.

Sin embargo, teniendo en cuenta las características ya mencionadas de las personas que cometen los *"delitos informáticos"*, estudiosos en la materia los han catalogado como "delitos de cuello blanco" término.([26]) introducido por primera vez por el criminólogo norteamericano **Edwin Sutherland** en el año de 1943.

Efectivamente, este conocido criminólogo señala un sinnúmero de conductas que considera como "delitos de cuello blanco", aún cuando muchas de estas conductas no están tipificadas en los ordenamientos jurídicos como delitos, y dentro de las cuales cabe destacar las *"violaciones a las leyes de patentes y fábrica de derechos de autor, el mercado negro, el contrabando en las empresas, la evasión de impuestos, las quiebras fraudulentas, corrupción de altos funcionarios, entre otros"*.

Asimismo, este criminólogo estadounidense dice que tanto la definición de los "delitos informáticos" como la de los "delitos de cuello blanco" no es de acuerdo al interés protegido, como sucede en los delitos convencionales sino de acuerdo al sujeto activo que los comete. Entre las características en común que poseen ambos delitos tenemos que: el sujeto activo del delito es una persona de cierto status socioeconómico, su comisión no puede explicarse por pobreza ni por mala habitación, ni por carencia de recreación, ni por baja educación, ni por poca inteligencia, ni por inestabilidad emocional.

Es difícil elaborar estadísticas sobre ambos tipos de delitos. La "cifra negra" es muy alta; no es fácil descubrirlo y sancionarlo, en razón del poder económico de quienes lo cometen, pero los daños económicos son altísimos; existe una gran

[26] DEL PONT K., Luis Marco y NADELSTICHER Mitrania, Abraham. Delitos de cuello blanco y reacción social. Instituto Nacional de Ciencias Penales. México. 1981.

indiferencia de la opinión pública sobre los daños ocasionados a la sociedad; la sociedad no considera delincuentes a los sujetos que cometen este tipo de delitos, no los segrega, no los desprecia, ni los desvaloriza, por el contrario, el autor o autores de este tipo de delitos se considera a sí mismos "respetables" otra coincidencia que tienen estos tipos de delitos es que, generalmente, son objeto de medidas o sanciones de carácter administrativo y no privativos de la libertad.

Por nuestra parte, consideramos que a pesar de que los "*delitos informáticos*" no poseen todas las características de los "delitos de cuello blanco", si coinciden en un número importante de ellas, aunque es necesario señalar que estas aseveraciones pueden y deben ser objeto de un estudio más profundo, que dada la naturaleza de nuestro objeto de estudio nos vemos en la necesidad de limitar.

2.7 SUJETO PASIVO DEL DELITO

En primer término tenemos que distinguir que *sujeto pasivo ó víctima del delito* **es el ente sobre el cual recae la conducta de acción u omisión que realiza el sujeto activo**, y en el caso de los "*delitos informáticos*" las víctimas pueden ser individuos, instituciones crediticias, gobiernos, etcétera que usan sistemas automatizados de información, generalmente conectados a otros.

El sujeto pasivo del delito que nos ocupa, es sumamente importante para el estudio de los "*delitos informáticos*", ya que mediante él podemos conocer los diferentes ilícitos que cometen los delincuentes informáticos, con objeto de prever las acciones antes mencionadas debido a que muchos de los delitos son

descubiertos casuísticamente por el desconocimiento del *modus operandi* de los sujetos activos.

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

Por lo anterior, se reconoce que *"para conseguir una prevención efectiva de la criminalidad informática se requiere, en primer lugar, un análisis objetivo de las necesidades de protección y de las fuentes de peligro. Una protección eficaz contra la criminalidad informática presupone ante todo que las víctimas potenciales conozcan las correspondientes técnicas de manipulación, así como sus formas de encubrimiento".*([27])

En el mismo sentido, podemos decir que mediante la divulgación de las posibles conductas ilícitas derivadas del uso de las computadoras, y alertando a las potenciales víctimas para que tomen las medidas pertinentes a fin de prevenir la delincuencia informática, y si a esto se suma la creación de una adecuada legislación que proteja los intereses de las víctimas y una eficiente preparación por parte del personal encargado de la procuración, administración y la

[27] http://www.monografia.com.

impartición de justicia para atender e investigar estas conductas ilícitas, se estaría avanzando mucho en el camino de la lucha contra la delincuencia informática, que cada día tiende a expandirse más.

Además, se debe destacar que los organismos internacionales han adoptado resoluciones similares en el sentido de que ***"educando a la comunidad de víctimas y estimulando la denuncia de los delitos se promovería la confianza pública en la capacidad de los encargados de hacer cumplir la ley y de las autoridades judiciales para detectar, investigar y prevenir los delitos informáticos"***.

2.8 PERFIL DEL DELINCUENTE

Como ya se ha dicha en múltiples ocasiones, este tipo de delito, al igual que la tecnología que se utiliza para su comisión y la persona que lo realiza, son nuevos en el ámbito criminal, por lo mismo, no se ajustan a la imagen estereotipada del delincuente (pobre, inculto, adicto a las drogas, etc.). No obstante que son muchos los casos, han sido pocas las denuncias precisamente por su falta de tipificación, sin embargo, con los datos empíricos existentes, se puede realizar un perfil del delincuente:

a) Son individuos que se caracterizan por no tener antecedentes penales y por haber desarrollado un modo de vida aparentemente adaptado sin una marcada agresividad, con una vida laboral y familiar estable.

b) El delincuente tiene un aspecto y un carácter agradables que le son necesarios para conquistar la confianza indispensable para una más fácil realización de su delito.

c) Es despierto, impaciente, muy motivado, audaz y aventurero; entre sus rasgos más acentuados se encuentra una imaginación exuberante, un sentido exagerado de la propia personalidad y una gran codicia.

d). Este tipo de delincuente es instruido y posee una inteligencia superior a la normal, por lo que para el representa un reto desactivar todas las medidas de seguridad que se va encontrando en el trayecto hacia la comisión del ilícito. cuanto más inteligente y mal intencionado sea el individuo, tanto mayor y sutil al daño que pueda ocasionar.

e). Por su comportamiento seguro, por la facilidad y naturalidad con que se expresa, por la forma en que viste, proyecta una imagen que representa un status social elevado. Esta imagen de solvencia que exhibe tiene el efecto de que se rechacen las sospechas hacia el.

f). A pesar de que este nuevo crimen ha proliferado, su comisión se hace posible a nivel de los empleados. Los nuevos sistemas de información son manejados por profesionales especialmente capacitados para ello, personas por lo general muy bien preparadas: Presidentes de las corporaciones, ingenieros en sistemas, programadores, analistas, etc.

Aunque el universo del criminal se reduce, pues no cualquiera puede cometer un delito informático ya que se requieren determinadas condiciones tales como

la preparación técnica, el acceso a los sistemas y el espíritu de aventura que representa el reto de enfrentarse a los dispositivos de seguridad de los programas de computación, existe un mayor numero de personas que ha recibido ahora la capacitación requerida para programar, penetrar y manipular los sistemas de computación. Además, por las ventajas que representa en cuanto a la cuantía que se puede obtener y a su impunidad por falta de tipificación, cada vez hay una mayor proliferación de expertos en informática de alto nivel.

Carlos Sarzana afirma que "la criminalidad de computadoras es cometida por la Élite de la delincuencia([28])".

Dentro de esta nueva delincuencia existen diferentes clases de individuos, tales como:

1. AMATEUR: Son gente ordinaria colocada en puesto. de confianza o con una experiencia obtenida por el manejo constante del equipo de computación que se encuentra en dificultades económicas por apuestas, drogas, etc. para la solución de sus problemas utiliza sus capacidades especiales violando la confianza en ellos depositada. Cabe aclarar que estos individuos no son necesariamente inteligentes, pero si expertos en las funciones propias de sus labores.

2. PROFESIONALES: Son personas sumamente inteligentes, cuentan con una preparación especial y generalmente están colocadas en puestos de alta dirección dentro de las corporaciones, como vicepresidentes, directores o

[28] LIMA. Ma. de la Luz. Op cit. P.35

gerentes. Precisamente por el puesto que desempeñan, se dan cuenta del valor de la información confidencial que manejan, por lo que conjuntado su inteligencia, experiencia en la operación de los sistemas de información y alta jerarquía, para ellos es relativamente fácil transferir, alterar o extraer, entre otras funciones, información contenida en la Unidad Central de Procesamiento de la computadora de la organización en la que laboran, obteniendo a cambio un enorme beneficio.

3. EXPLORADORES DE SISTEMAS: por lo regular, son estudiantes de universidades que nunca han sido arrestados; no son extremistas ni terroristas; tampoco son vándalos o saboteadores. Son intrusos atrevidos que no buscan destruir nada ni tampoco les interesa la información contenida en los sistemas a los que se accedan; lo único que pretenden es traspasar la tecnología, demostrar su superioridad sobre los complejos controles de seguridad que guardan a estos sistemas y que su hazaña sea reconocida. Su intrusión a los sistemas es el reto; que su logro se haga publico reconociendo su inteligencia suprema, es su recompensa.

4. PARTIDARIOS EXTREMISTAS: Son personas que se dedican a luchar por los derechos humanos y por sus ideales políticos, económicos y religiosos. Por lo regular, están involucrados en actividades criminales y son protegidos por pequeños grupos rebeldes. Se les conoce como extremistas o terroristas, pero son diferentes a las corporaciones criminales organizadas, pues ellos se dedican a cambiar positivamente a la sociedad.

Este cambio implica el ataque a las multinacionales e identifican a las computadoras como instrumentos de estas debido al monopolio que ejercen en

los sistemas computacionales. Afirman que el sector electrónico es el sector estratégico del avance del capitalismo, pues no sólo exportan su alta tecnología, sino también su ideología, idioma y cultura y a través de las redes de computación realizan un espionaje total sobre las personas.

5. ORGANIZACIONES CRIMINALES: La mafia es el prototipo del crimen organizado. Estas, aparte de utilizar las computadoras en sus negocios a gran escala como son sus operaciones financieras con los bancos o con los corredores de apuestas y de drogas, las utilizan para cometer otros delitos en contra de organizaciones que cuentan con sistemas de cómputo como herramienta de trabajo. El crimen organizado está utilizando la computadora como una arma muy poderosa y efectiva.

En cuanto a las víctimas, el universo se amplia, pues la dependencia de la nueva tecnología nos hace más susceptibles de convertirnos en víctimas.

Sin embargo, al contrario de cualquier persona denunciaría, a estas instituciones preocupan dichas infracciones, pues cuentan con partidas presupuéstales previamente creadas precisamente para tales desfalcos, por lo que no denuncian dichas conductas ilícitas.

Sin embargo, no todas las personas afectadas por estos delitos cuentan con la misma capacidad de absorción de semejantes perdidas, no obstante, al no estar tipificada esta acción ilícita, el sujeto pasivo queda imposibilitado de exigir justicia y que se castigue al delincuente, ya que como están las cosas actualmente, este, a pesar de saber quien se está beneficiando en su perjuicio y

como lo está haciendo, queda impotente de activar el órgano de la justicia, pues no hay delito que perseguir por la propia ausencia de tipo y el sujeto activo queda en libertad y en posibilidad de continuar delinquiendo.([29])

2.9 PROBLEMATICA LOS *HACKERS* EN LA SOCIEDAD

Tenemos el problema de los llamados *hackers*, que son genios en materia de computación, que cuentan con programas, y con la habilidad suficiente, para penetrar a computadoras y redes de cómputo con sistemas de seguridad "supuestamente" muy buenos como lo son las computadoras del pentágono, la CIA y el FBI; pueden checar las transacciones que realizan diversas personas con sus tarjetas de crédito, los montos, así como sus claves; pueden desviar llamadas a través de diversos satélites para no ser detectados, pueden penetrar a la red Internet, sin que se les cobre, pues hacen de algún modo inrrastreable su ubicación o su penetración; pueden crear números falsos de tarjetas de crédito; realizar fraudes, etc([30]).

Cómo ya se menciono con anterioridad, la falta de preparación de las personas a cargo de las redes computacionales, las hace muy vulnerables a la introducción de personas ajenas a éstas, como lo son los *hackers*, como lo es la introducción de virus informáticos debido a negligencia, etc.

---

[29] MARCHIORI, Hilda, " Personalidad del delincuente" , 3ra. México , ed. Porrua, 1985. P 36

[30] DE LA CUADRA, Enrique. "Regulación jurídica de la informática computacional" Temas de Derecho Año II No. 3, 1987. Universidad Gabriela Mistral. Santiago de Chile, p. 1-4.

Bien, tenido esto en cuenta, resulta que la responsabilidad de los administradores de una red de cómputo puede ser de dos tipos, en mi opinión:

1. CULPABLE: Es imputable al Administrador de la red de cómputo, si siendo éste un Ingeniero en Sistemas Computacionales, y contando con los cursos de certificación para operar dicho sistema de red, obra sin la diligencia debida, si solapa la intromisión de *hackers*, sin no ve por mantenerse preparado para manejar el sistema de red, o si no tiende a mantener la red en óptimas condiciones, es decir libre de virus. Si obra dolosamente o si perpetra el mismo ilicito.

2. NO CULPABLE: No es imputable al Administrador de la red de cómputo, si este no es Ingeniero en Sistemas Computacionales, o si no cuenta con la debida capacitación para operar un sistema de red. Esto puede ser debido a la negligencia de los Administradores de la Empresa para contratar a la gente idónea para realizar el trabajo de Administradores de Red, como lo serían los Ingenieros en Sistemas Computacionales, si no les proporcionan los medios de capacitación para operar el sistema de red, o si no les proporcionan los medios para conseguir los programas mínimos indispensables para mantener adecuadamente la red, como lo serían los antivirus, versiones nuevas de la red, etc.

En este caso de la responsabilidad no imputable al Administrador de redes de cómputo, el responsable será la empresa, o el propietario de la red.

Serán responsables de los daños que se causen por la indebida destrucción, apoderamiento, modificación, o utilización de archivos que pertenezcan a los usuarios de modo personal.

¿Cómo Operan?

Los hackers son personas así llamadas que hacen uso de diversos programas, para penetrar en las redes computacionales, usurpando cuentas de usuarios, creando nuevas cuentas, o utilizando cuentas predeterminadas por el sistema de red. Estos programas con los que cuentan los *hackers*, pueden obtenerse sin mayor esfuerzo, en la autopista de información, mejor conocida como Internet.([31])

Hay diversas opiniones respecto de la rastreabilidad o inrrastreabilidad de estos criminales.

¿Es posible rastrearlos?

En cuanto su inrrastreabilidad, el Lan Times, el 8 de febrero de 1993, señalaba "tips" para el rastreo de *Hackers*, como los siguientes:

(1) EN LO INTERNO: Mientras se intenta interrumpir en una red a través de una línea privada de intercambio *(Private branch exchange)*, los *hackers* se delatarán pues al utilizar los llamados "*war dialers*" (programas de PC diseñados para romper códigos de contraseñas así como para buscar números de la serie

[31] DE LA CUADRA Enrique. Op. Cit p. 7

800) dejan detrás una infinidad de números de contraseñas equivocadas de usuarios.

(2) EN LO EXTERNO: En el camino de salida de un sistema, los *hackers* se delatarán por utilizar extensiones fantasmas, códigos de acceso raramente utilizados, etc.

(3) CODICIA: Cuando los *hackers* son realmente buenos, no dejarán huellas exceptuando la codicia. Estos *hackers* son revelados por la utilización de patrones que se desvían de los hábitos normales de negociación.

(4) CAMBIOS DE SISTEMAS: El daño más potencial existe cuando la programación de los sistemas es cambiada para facilitar la actividad de los *hackers (hacking)*.

Cualquiera tomando contraseñas para la línea privada de intercambio del puerto de mantenimiento de la computadora, o uso no autorizado debe ser rastreado, y detenido inmediatamente. Aquí es dónde los administradores de redes LAN y de redes de telecomunicaciones deben trabajar como un equipo.

Simon Gardner, en un artículo de la revista europea electrónica FUTURE NET, del mes de Enero de 1995, establece las siguientes reglas de los *Hackers:*

(1) Si realmente lo quieren, lo obtendrán.

(2) Siempre hay más de una manera de entrar.

(3) Demasiada seguridad puede ser tan mala como no tener la suficiente.

Medidas de seguridad.

Gardner menciona que una manera de hacer más difícil el acceso a los *hackers*, es el hecho de que los administradores de redes, borren o quiten las contraseñas predeterminadas de las redes a su encargo, desafortunadamente, señala que es muy poca la gente que toma esta precaución.
Señala también Simon Gadner, que desgraciadamente los *hackers* descubren prácticamente de manera inmediata la manera de burlar los nuevos sistemas de seguridad como los de los de encriptamiento de archivos, etc.

El hecho de que los administradores de las redes de cómputo sean Ingenieros en sistemas Computacionales, y que cuenten con los conocimientos certificados para la adecuada operación del Sistema en red, así como el conocimiento de sus puntos débiles, les permitiría hacer un poco más complicado el acceso a este tipo de criminales([32]).

2.10 LA ÉTICA Y EL DERECHO INFORMATICO

Ética (del griego ethika, de ethos, comportamiento, costumbre), principios o pautas de la conducta humana, a menudo y de forma impropia llamada moral (del latín mores, costumbre) y por extensión, el estudio de esos principios a veces llamado filosofía moral.

[32] Hackers. Historias prohibidas. Revista Electrónica en Español WORLD.

La ética como una rama de la filosofía, está considerada como una ciencia normativa, porque se ocupa de las normas de la conducta humana, y para distinguirse de la ciencias formales, como las matemáticas y la lógica, y de las ciencias empíricas, como la química y la física. Las ciencias empíricas sociales, sin embargo, incluyendo la psicología, chocan en algunos puntos con los intereses de la ética ya que ambas estudian la conducta social. Por ejemplo, las ciencias sociales a menudo procuran determinar la relación entre principios éticos particulares y la conducta social, e investigar las condiciones culturales que contribuyen a la formación de estos principios.([33])

Los filósofos han intentado determinar la bondad en la conducta de acuerdo con dos principios fundamentales y han considerado algunos tipos de comportamiento buenos en sí mismo o buenos por que se adoptan a un modelo moral.

El primero implica un valor final deseable en sí mismo y no sólo como un medio para alcanzar un fin. En la historia de la ética hay cuatro modelos de conducta principales, cada uno de los cuales ha sido propuesto por varios grupos o individuos como el bien mas elevado, la felicidad o placer, el deber, la virtud o la obligación y la perfección, el más completo desarrollo de las potencialidades humanas. Dependiendo del marco social, la autoridad invocada para una buena conducta es la voluntad de una deidad, el modelo de la naturaleza o el dominio de la razón. Cuando la voluntad de una deidad es la autoridad, la obediencia a los mandamientos divinos o a los textos bíblicos, supone la pauta de conducta aceptada. Si el modelo de autoridad es la naturaleza, la pauta es la conformidad

[33]Código de Etica y Conducta Profesional de la Academia Mexicana de Informática citado por Alexander Díaz García (Elementos de la Informática Jurídica).

con las cualidades atribuidas a la naturaleza humana. Cuando rige la razón, se espera que la conducta moral resulte del pensamiento racional.

Desde que los hombres viven en comunidad la regulación moral de la conducta ha sido necesaria para el bienestar colectivo. Aunque los distintos sistemas morales se establecían sobre pautas arbitrarias de conducta, evolucionaron a veces de forma irracional , a partir de que se violaran los tabúes religiosos o de conductas que primero fuerón hábito y luego costumbre, o asimismo de leyes impuestas por líderes para prevenir desequilibrios en el seno de la tribu. Incluso las grandes civilizaciones clásicas Egipcias y Sumeria desarrollaron éticas no sistematizadas, cuyas máximas y preceptos eran impuestos por líderes seculares como Ptahhotep y estaban mezclados con una religión estricta que afectaba la conducta de cada Egipcio con cada Sumerio. En la China clásica las máximas de Confucio fuerón aceptadas como código moral. Los filósofos griegos desde el siglo VI a.c., teorizaron mucho sobre la conducta moral, lo que llevó al posterior desarrollo de la ética como una filosofía.

Después de este prolegómeno histórico y etimológico, me centraré en el tema que me ha motivado ha investigar, para hablarles cómo nos afecta la irracionalidad moral de algunos en el derecho informático, siendo un problema serio en esta nueva tecnología, como es llamada la materia en Europa.

La relación existente entre el Derecho y la Informática se podría apreciar desde dos ópticas: si lo tomamos desde el punto de vista instrumental, hacemos referencia a la informática jurídica, pero si lo observamos como objeto del Derecho, hemos de entenderlo como Derecho Informático.

La coexistencia de estas dos disciplinas funcionan eficiente y eficazmente, en razón a que el derecho es ayudado por la informática; no obstante lo anterior estas deben estar sometidas a ciertas normas y/o criterios globalizados, para asegurar su cumplimiento y respeto de las pautas informáticas. Efectivamente, al surgir el derecho informático como una ciencia que surge en razón de la cibernética, como ciencia que trata la relación derecho e informática desde el punto de vista del conjunto de normas, doctrina y jurisprudencia, que van a establecer, regular las acciones, procesos, aplicaciones, relaciones jurídica, en su complejidad de la informática. Pero del otro lado encontramos a la informática jurídica que ayudada por el derecho informático hace válida esa cooperación de la informática al derecho.

Poco a poco se ha abandonado la idea que la informática es pura y llanamente, la utilización de aparatos o elementos físicos electrónicos; por ello se torna improcedente, que sea juzgada por su simple exterioridad. Es una perogrullada afirmar que de las relaciones Ínter subjetivas de las personas naturales o jurídicas y de entes morales del Estado, surgen reglas técnicas conectadas con el derecho, constituyendo esto, entonces en los medios para la realización de sus fines, ética y legalmente permitidos, creando principios y conceptos que institucionalizan la Ciencia Informática, con autonomía propia. Esos principios conforman las directrices propias de la institución informática y vienen a constituir las pautas de la interrelación nacional-universal, con normas mundiales supra nacional y cuyo objeto será necesario recoger mediante tratados públicos que hagan posible el proceso comunicacional en sus propios fines con validez y eficacia universal. Por lo tanto, la informática jurídica puede ser considerada como fuente del derecho, criterio propio que tal vez encuentre muchos tropiezos debido a la falta de cultura informática que existe en nuestro país.

La informática presenta a los usuarios de los PC, una serie de problemas relacionados con la ética y los valores tal como ninguna otra área del derecho lo ha hecho en el pasado. Hasta ahora, la aplicación de los conocimientos adquiridos en situaciones de dilema moral se ha limitado a lo ficticio o casos hipotéticos o a lo ejemplar, casos tipo, y por lo tanto las oportunidades de hacer el mal siempre han rondado lo teórico, con la única excepción de lo referido a las relaciones interpersonales y sociales. En la informática, las cuestiones éticas se plantean a cada segundo. ¿Se puede leer el correo electrónico de otras personas? ¿Está bien borrar archivos ajenos? ¿Es lícito utilizar software sin pagarlo? ¿Es aceptable copiar la información producida por otros? ¿Se podrán instalar programas en los computadores ajenos? ¿O un virus? ¿Estará mal interferir en otros sistemas a través de la red? ¿Puede el funcionario o empleado judicial hacer cualquier cosa que le venga en voluntad con el computador puesto por el Estado a su disposición? Lo importante a estas preguntas es que no sólo se pueden hacer en su casa u oficina, sino que el usuario tiene el poder concreto de elegir entre el bien y el mal y la posibilidad real de hacerlo, en muchos casos sin ver cómo afecta a otras personas (lo cual disminuye invariablemente la culpabilidad, cuando no la anula por completo) y con una apreciable impunidad como se sabe ocurre en México, por ausencia de una verdadera política criminal informática.

Asociados a las reglas de uso ético de una sistema informático está el conocimiento de cómo operarlo. Si analizamos el modo en que este conocimiento se adquiere en la vida real, veremos que casi siempre es previo a la consideración de sus efectos. En un escenario constructivista, por ejemplo su oficina, el incipiente informático aprende a crear, copiar, modificar y borrar archivos prácticamente sin darse cuenta, porque esas habilidades son poco menos que la base operativa de un sistema computacional, y recién después de esto descubre lo

que significa tener el poder de aplicar ese saber sobre la producción ajena. Lo mismo sucede con la Internet donde es posible un anónimo y es muy tentador hacer travesuras a diestra y siniestra enviando correo electrónico o armando páginas web con contenido dudoso. No por nada los más temibles *hacker*, palabra tomada del inglés hack (hachar) que se aplicaba a quienes reparaban teléfonos y abrían las cajas a golpes, son a menudo impúberes, expertos autodidacta en informática, pero perfectos ignorantes del derecho ajeno.

Dificultades como éstas apuntan directamente al corazón de la didáctica de la computación: ¿Cuándo, cómo y a quién debe enseñarse a hacer aquello potencialmente dañino para un sistema de cómputos o para personas al utilizarlo? Los principios generales de ética y moral deben tener un origen de cuna y los maestros en la escuela ofrecerán, amén de una excelente enseñanza técnica, un fortalecimiento de estos valores adecuándolos a la informática. En muchos sentidos es loable estimular la curiosidad infantil, pero ¿hasta qué punto se pude admitir que el niño tenga poder sobre un sistema, como el de la escuela, cuya integridad es vital para enseñar y aprender, antes de tener una noción más o menos clara del alcance de sus actos? Es muy frecuente en situaciones reales, tener que suspender la lección porque un alumno ha desconectado la red o su terminal, tras borrar archivos esenciales por descuido o torpeza, y cuando el docente, se inclina sobre el teclado y supera el problema, aquellos los más precoces, pícaramente están pensando "de modo que así es como se puede interrumpir la clase". Cuando no se ha formado una clara noción de lo que es ético hacer con una computadora, hasta la curiosidad más simple, puede ser el preludio de un acto doloso. No sería mala la idea recuperar en la escuela la costumbre de que los niños pidan permiso antes de hacer algo con el equipo. Enseñar a los alumnos nociones clave de ética actual, de una forma práctica

desde luego, que insista en el problema del conflicto ético, los resultados serian razonablemente exitosos. Comprender conceptos de la ética actual como la idea de bien público o cómo todo el edificio ético ha de estar construido en la igualdad de oportunidades, serían perfectos para desarrollar un sentido de responsabilidad social en informáticos, abogados e ingenieros El conocimiento es una via directa hacia el poder, pero quien sabe hacer algo tiene que tener primero en claro en qué casos debe hacerse y en qué casos no; sus sentimientos y reflexión sobre el concepto de responsabilidad deberá imperar.

Ahora bien, superada la primera etapa del hombre, su formación académica y solidificación de principios y valores, pasaremos a hablar de las implicaciones que tienen las nuevas tecnologías al servicio de los individuos. Gracias a la Internet, disponemos por primera vez de medios globales de comunicación a precios ridículos y por ello se ha masificado su uso, paulatinamente está ocurriendo en México, por cierto ocupa un lugar preferencial en Latinoamérica después de Colombia, Argentina y Brasil. La red es una parte cada vez más importante de nuestras vidas y esa tendencia sólo va a incrementarse en el futuro, con la ayuda directa del Estado. Es muy importante evitar que Internet se desarrolle solamente desde patrones económicos y lo ideal sería que la red continué siendo un espacio propio y diverso, una espacio único que sea diferente a los medios de comunicación de masa o a un inmenso centro comercial, pero también deben existir normas, no sólo legales, sino éticas también principalmente, pues la guerra del libre mercado hacen superar muchas veces el limite de lo ético.([34])

[34] Código de Etica y Conducta Profesional de la Academia Mexicana de Informática. www.amiac.cm.

Es necesario que nos enfrentemos a la tendencia de mercantilizar la Red ¿Cómo hacerlo? Considero que todo descansa sobre dos pilares: diversidad y responsabilidad social. Todos los científicos tienen una responsabilidad social.

La tecnología se usa en el mundo y el científico y el ingeniero han de olvidarse de la torre de marfil y recordar que sus inventos se van a utilizar de muchas formas. Muchas veces se usarán de manera contrarias a nuestros derechos y libertades. El software y el hardware se han de diseñar y montar pensando en el concepto de diversidad. Evitar los caminos cerrados, permitir que programas y maquinaria se usen de la forma más abierta y diversa posible, pero no ilimitada, permitirá una convivencia sana, armoniosa y respetuosa.

No podemos olvidar que en cierto momento de nuestras vidas, un informático tendrá que plantearse, como ya lo hacen los abogados, médicos, biólogos, y físicos, si quiere realmente desarrollar un proyecto que claramente se va a usar para menoscabar los derechos de los internáutas. ¿Puede un abogado informático con convicciones de ética, sugerirle a su cliente que instale un puerta trasera en un navegador de manera que todas las operaciones que realice con él queden registradas, para venderlas como manipular datos sensibles o simplemente confidenciales, abusando del derecho a la privacidad del usuario? No resulta difícil responder rotundamente no.

Otra cosa es la situación personal de cada uno y uno en cada momento decidirá qué puede y que no puede hacer, no obstante invito al auditorio a no participar en cualquier proyecto o desarrollo que implique poner en peligro las libertades y derechos de los ciudadanos, tanto a nivel oficial como en su vida particular.

2.11 CLASIFICACIÓN DE LOS DELITOS INFORMATICOS

Julio Téllez Valdés clasifica a los delitos informáticos en base a dos criterios: como instrumento o medio, o como fin u objetivo.([35])

1. Como instrumento o medio:
Se tienen a las conductas criminógenas que se valen de las computadoras como método, medio, o símbolo en la comisión del ilícito.

2. Como fin u objetivo:
En esta categoría se enmarcan las conductas criminógenas que van dirigidas en contra de la computadora, accesorios o programas como entidad física.

María de la Luz Lima, presenta una clasificación, de lo que ella llama "*delitos electrónicos*", diciendo que existen tres categorías, a saber:

Los que utilizan la tecnología electrónica como método,
Los que utilizan la tecnología electrónica como medio y
Los que utilizan la tecnología electrónica como fin.

Como método- conductas criminógenas en donde los individuos utilizan métodos electrónicos para llegar a un resultado ilícito.
Como medio.- conductas criminógenas en donde para realizar un delito utilizan una computadora como medio o símbolo.
Como fin.- conductas criminógenas dirigidas contra la entidad física del objeto o máquina electrónica o su material con objeto de dañarla. ([36])

[35] TELLEZ Valdés. Julio Op cit. P.103

2.12 TIPOS DE DELITOS INFORMATICOS Y SUS CARACTERÍSTICAS

Tipos de delitos informáticos reconocidos por Naciones Unidas

DELITO	CARACTERÍSTICAS
Fraudes cometidos mediante manipulación de computadoras.	
"Manipulación de los datos de entrada	"Este tipo de fraude informático conocido también como sustracción de datos. representa el delito informático más común ya que es fácil de cometer y difícil de descubrir. Este delito no requiere de conocimientos técnicos de informática y puede realizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos en la fase de adquisición de los mismos.
La manipulación de programas	Es muy difícil de descubrir y a menudo pasa inadvertida debido a que el delincuente debe tener conocimientos técnicos concretos de informática. Este delito consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas. Un método común utilizado por las personas que tienen conocimientos especializados en programación

[36] http://tiny.uasnet.mx/index.htm

informática es el denominado Caballo de Troya, que consiste en insertar instrucciones de computadora de forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal.

Manipulación de los datos de salida

Se efectúa fijando un objetivo al funcionamiento del sistema informático. El ejemplo más común es el fraude de que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos. Tradicionalmente esos fraudes se hacían a base de tarjetas bancarias robadas, sin embargo, en la actualidad se usan ampliamente equipo y programas de computadora especializados para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito.

Fraude efectuado por manipulación informática

Aprovecha las repeticiones automáticas de los procesos de cómputo. Es una técnica especializada que se denomina "técnica del salchichón" en la que "rodajas muy finas" apenas perceptibles, de transacciones financieras, se van sacando repetidamente de una cuenta y se transfieren a otra.

Falsificaciones informáticas

Como objeto	Cuando se alteran datos de los documentos almacenados en forma computarizada.
Como instrumentos	Las computadoras pueden utilizarse también para efectuar falsificaciones de documentos de uso comercial. Cuando empezó a disponerse de fotocopiadoras computarizadas en color a base de rayos láser surgió una nueva generación de falsificaciones o alteraciones fraudulentas. Estas fotocopiadoras pueden hacer copias de alta resolución, pueden modificar documentos e incluso pueden crear documentos falsos sin tener que recurrir a un original, y los documentos que producen son de tal calidad que sólo un experto puede diferenciarlos de los documentos auténticos.

Daños o modificaciones de programas o datos computarizados

Sabotaje informático	Es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema. Las técnicas que permiten cometer sabotajes informáticos son:
Virus	Es una serie de claves programáticas que pueden adherirse a los programas legítimos y propagarse a otros programas informáticos. Un virus puede ingresar en un

	sistema por conducto de una pieza legitima de soporte lógico que ha quedado infectada, así como utilizando el método del Caballo de Troya.
Gusanos	Se fabrica de forma análoga al virus con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse. En términos médicos podría decirse que un gusano es un tumor benigno, mientras que el virus es un tumor maligno. Ahora bien, las consecuencias del ataque de un gusano pueden ser tan graves como las del ataque de un virus: por ejemplo, un programa gusano que subsiguientemente se destruirá puede dar instrucciones a un sistema informático de un banco para que transfiera continuamente dinero a una cuenta ilícita.
Bomba lógica o cronológica	Exige conocimientos especializados ya que requiere la programación de la destrucción o modificación de datos en un momento dado del futuro. Ahora bien, al revés de los virus o los gusanos, las bombas lógicas son difíciles de detectar antes de que exploten; por eso, de todos los dispositivos informáticos criminales, las bombas lógicas son las que poseen el máximo potencial de daño. Su detonación puede programarse para que cause el máximo de daño y para que tenga lugar mucho tiempo después de

	que se haya marchado el delincuente. La bomba lógica puede utilizarse también como instrumento de extorsión y se puede pedir un rescate a cambio de dar a conocer el lugar en donde se halla la bomba.
Acceso no autorizado a servicios y sistemas informáticos	Por motivos diversos: desde la simple curiosidad, como en el caso de muchos piratas informáticos *(hackers)* hasta el sabotaje o espionaje informático.
Piratas informáticos o hackers	El acceso se efectúa a menudo desde un lugar exterior, situado en la red de telecomunicaciones, recurriendo a uno de los diversos medios que se mencionan a continuación. El delincuente puede aprovechar la falta de rigor de las medidas de seguridad para obtener acceso o puede descubrir deficiencias en las medidas vigentes de seguridad o en los procedimientos del sistema. A menudo, los piratas informáticos se hacen pasar por usuarios legítimos del sistema; esto suele suceder con frecuencia en los sistemas en los que los usuarios pueden emplear contraseñas comunes o contraseñas de mantenimiento que están en el propio sistema.

reproducción no autorizada de programas informáticos de protección legal	Esta puede entrañar una pérdida económica sustancial para los propietarios legítimos. Algunas jurisdicciones han tipificado como delito esta clase de actividad y la han sometido a sanciones penales. El problema ha alcanzado dimensiones transnacionales con el tráfico de esas reproducciones no autorizadas a través de las redes de telecomunicaciones moderna. Al respecto, considero, que la reproducción no autorizada de programas informáticos no es un *delito informático* debido a que el bien jurídico a tutelar es la propiedad intelectual."([37])

[37] NACIONES UNIDAS. Revista Internacional de Política Criminal. Manual de las Naciones Unidas sobre Prevención del Delito y Control de delitos informáticos. Oficina de las Naciones Unidas en Viena. Centro de Desarrollo Social y Asuntos humanitarios. Nos.43 y 44. Naciones Unidas. Nueva York.1994.

CAPITULO III

MÉXICO Y SU SITUACIÓN ACTUAL CON LA INFORMÁTICA JURÍDICA

3.1 LA IMPORTANCIA DE LA INFORMATICA EN LOS ULTIMOS AÑOS

Como ustedes saben, la convergencia de la computación, de la microelectrónica y de las telecomunicaciones conforman lo que en la actualidad se denomina informática. Esta ha permitido producir y manejar información en grandes volúmenes y consultarla y transmitirla a enormes distancias y en tiempos muy reducidos.

Particularmente en los últimos diez años la informática ha irrumpido en el mundo y ha ido penetrando en todos y cada uno de los aspectos de la vida cotidiana. Ha influido en múltiples actividades económicas y en las esferas políticas y sociales. Incluso ha modificado el uso del tiempo de millones de personas y la forma de vida de la sociedad contemporánea.([38])

De hecho, estamos viviendo un cambio hacia lo que ya se conoce como la Sociedad de la Información, de la cual la informática constituye la infraestructura fundamental.

En dicha sociedad, el adecuado uso y aprovechamiento de la informática brinda múltiples beneficios para las naciones.

---

[38] HANCE. Olivier. Leyes y Negocios en Internet. México. De. Mc Graw Hill Sociedad Internet. México. 1996. p 7.

3.2 CONTRIBUCIONES DE LA INFORMÁTICA AL DESARROLLO NACIONAL

La informática contribuye a fortalecer el ejercicio pleno de nuestra soberanía. A través de su empleo es posible realizar un seguimiento preciso y detallado de las características físicas del territorio, elemento consustancial y primigenio de nuestra nación. Su uso ofrece además, la posibilidad de ampliar y consolidar la presencia de México en el mundo y de reforzar la cultura e identidad nacionales.

Esta tecnología también puede apoyar en la consolidación de un país de leyes y de justicia, al aportar instrumentos valiosos para la aplicación de la ley y para garantizar el orden público. Asimismo, al acrecentar las posibilidades de acceso a la información, permite una sociedad más consciente y con mayores oportunidades de participación en todas las actividades de la vida nacional. Por eso existe una alta y positiva correlación entre el desarrollo democrático de un país y su desarrollo informático.

La informática apoya al nuevo federalismo al contribuir en los procesos de redistribución de competencias, responsabilidades y capacidades de decisión entre los tres órdenes de gobierno de la República. Con ello, coadyuva al fortalecimiento de los estados y de sus municipios, células básicas del tejido que da forma y sustento al pacto de unidad de los mexicanos.

Además, propicia el desarrollo social, al apoyar funciones estratégicas de las instituciones y sectores que ofrecen servicios en materia de educación, salud, entre otros.

También contribuye a las tareas de ordenamiento territorial y ecológico, y a las acciones de administración del territorio para el desarrollo urbano y rural, repercutiendo favorablemente en los niveles de bienestar de la población.([39])

Asimismo, la informática constituye una infraestructura fundamental para el desempeño de la economía nacional. Incluso, en el mundo globalizado de hoy, el adecuado uso de ésta es indispensable para que los sectores productivos sean competitivos.

Ejercicio pleno de la soberanía, Estado de Derecho, Desarrollo Democrático, Bienestar Social y Crecimiento Económico son todos, objetivos nacionales en cuyo logro la informática puede contribuir de manera decisiva.([40])

Consecuentemente, la informática no debe ser vista como una herramienta de uso exclusivo de especialistas de aplicación aislada y estrictamente técnica, sino como un elemento de la mayor trascendencia para el presente y para el futuro.

La informática en el Plan Nacional de Desarrollo 1995-2001 y el Programa de Desarrollo Informático

Dada su importancia estratégica, el propio Plan Nacional de Desarrollo 1995-2001 señala en forma explícita, las directrices para promover el desarrollo de la informática en nuestro país.

---

[39] www.netle-ec.com.
[40] GARCÍA Fabián y Pablo Palazzi. Consideraciones para una reforma penal en materia de seguridad y virus informáticos. Ponencia presentada en España en 1995.

Asi, el Plan hace referencia a la generación y difusión de las innovaciones tecnológicas, a su aprovechamiento en todos los sectores, y al establecimiento de mecanismos para asegurar la coordinación de las actividades relativas a las tecnologias de la información en el ámbito nacional.

Incluso el Plan establece, en el contexto de los programas especiales y sectoriales, la conformación de un Programa de Desarrollo Informático, el cual fué elaborado mediante una amplia consulta popular, ya fué presentado y se encuentra en su fase de instrumentación.

Dicho Programa, con horizonte al año 2001, señala, entre sus múltiples objetivos, contar con disposiciones jurídicas relativas a la informática, que aseguren las condiciones requeridas para su mejor aprovechamiento. ([41])

Considerando el carácter estratégico de la informática, considerando los objetivos enunciados en el Plan Nacional de Desarrollo, y considerando las estrategias definidas en el Programa de Desarrollo Informático, unos de los objetivos por el cual se lleva acabo estos programas es recopilar opiniones, propuestas y experiencias en torno al marco jurídico relativo al uso y al desarrollo de la informática en los últimos días.

---

[41] Prevención del delito y justicia penal en el desarrollo informatico nacional: . Documento de trabajo preparado por la Secretaria (A/CONF.144/5). Octavo Congreso sobre Prevención del delito y tratamiento del delincuente. Guadalajara 2001.

3.3 ORGANISMOS INTERNACIONALES EN LA INFORMÁTICA Y EL DERECHO

El objetivo de este tema es presentar todos aquellos elementos que han sido considerados tanto por organismos gubernamentales internacionales así como por diferentes Estados, para enfrentar la problemática de los *delitos informáticos* a fin de que contribuyan al desarrollo de este trabajo.

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

En un primer término, debe considerarse que en 1983, la **Organización de Cooperación y Desarrollo Económico (OCDE)** inició un estudio de la posibilidad de aplicar y armonizar en el plano internacional las leyes penales a fin de luchar contra el problema del uso indebido de los programas computacionales.[42]

Las posibles implicaciones económicas de la delincuencia informática, su carácter internacional y, a veces, incluso transnacional y el peligro de que la diferente protección jurídico-penal nacional pudiera perjudicar el flujo internacional de información, condujeron en consecuencia a un intercambio de opiniones y de propuestas de solución. Sobre la base de las posturas y de las deliberaciones surgió un análisis y valoración comparativista de los derechos nacionales aplicables así como de las propuestas de reforma. Las conclusiones

[42] http://rtn.net.mx/ocde/index.html.

político-jurídicas desembocaron en una lista de las acciones que pudieran ser consideradas por los Estados, por regla general, como merecedoras de pena.

De esta forma, la **OCDE** en 1986 publicó un informe titulado ***Delitos de Informática: análisis de la normativa jurídica***, en donde se reseñaban las normas legislativas vigentes y las propuestas de reforma en diversos Estados Miembros y se recomendaba una lista mínima de ejemplos de uso indebido que los países podrían prohibir y sancionar en leyes penales *(Lista Mínima)*, como por ejemplo el fraude y la falsificación informáticos, la alteración de datos y programas de computadora, sabotaje informático, acceso no autorizado, interceptación no autorizada y la reproducción no autorizada de un programa de computadora protegido.

La mayoría de los miembros de la Comisión Política de Información, Computadores y Comunicaciones recomendó también que se instituyesen protecciones penales contra otros usos indebidos *(Lista optativa o facultativa)*, espionaje informático, utilización no autorizada de una computadora, utilización no autorizada de un programa de computadora protegido, incluido el robo de secretos comerciales y el acceso o empleo no autorizado de sistemas de computadoras.

Con objeto de que se finalizára la preparación del informe de la **OCDE**, el Consejo de Europa inició su propio estudio sobre el tema a fin de elaborar directrices que ayudasen a los sectores legislativos a determinar qué tipo de conducta debía prohibirse en la legislación penal y la forma en que debía conseguirse ese objetivo, teniendo debidamente en cuenta el conflicto de intereses entre las libertades civiles y la necesidad de protección.

La lista mínima preparada por la **OCDE** se amplió considerablemente, añadiéndose a ella otros tipos de abuso que se estimaba merecían la aplicación de la legislación penal. El Comité, Especial de Expertos sobre Delitos relacionados con el empleo de las computadoras, del Comité Europeo para los problemas de la Delincuencia, examinó esas cuestiones y se ocupó también de otras, como la protección de la esfera personal, las víctimas, las posibilidades de prevención, asuntos de procedimiento como la investigación y confiscación internacional de bancos de datos y la cooperación internacional en la investigación y represión del *delito informático*.

Una vez desarrollado todo este proceso de elaboración de las normas a nivel continental, el Consejo de Europa aprobó la recomendación R(89)9 sobre delitos informáticos, en la que se "recomienda a los gobiernos de los Estados miembros que tengan en cuenta cuando revisen su legislación o preparen una nueva, el informe sobre la delincuencia relacionada con las computadoras .... y en particular las directrices para los legisladores nacionales". Esta recomendación fué adoptada por el Comité de Ministros del Consejo de Europa el 13 de septiembre de 1989.

Las directrices para los legisladores nacionales incluyen una lista mínima, que refleja el consenso general del Comité, acerca de determinados casos de uso indebido de computadoras y que deben incluirse en el derecho penal, así como una lista facultativa que describe los actos que ya han sido tipificados como delitos en algunos Estados pero respecto de los cuales no se ha llegado todavía a un consenso internacional en favor de su tipificación.

Adicionalmente, en 1992, la **OCDE** elaboró un conjunto de normas para la seguridad de los sistemas de información, con intención de ofrecer las bases para

que los Estados y el sector privado pudieran erigir un marco de seguridad para los sistemas informáticos el mismo año.

En este contexto, consideramos que si bien este tipo de organismos gubernamentales ha pretendido desarrollar normas que regulen la materia de *delitos informáticos*, ello es resultado de las características propias de los países que los integran, quienes, comparados con México u otras partes del mundo, tienen un mayor grado de informatización y han enfrentado de forma concreta las consecuencias de ese tipo de delitos.

Por otra parte, a nivel de organizaciones intergubernamentales de carácter universal, debe destacarse que en el seno de la **Organización de las Naciones Unidas (ONU)**, en el marco del Octavo Congreso sobre Prevención del Delito y Justicia Penal, celebrado en 1990 en la Habana, Cuba, se dijo que la delincuencia relacionada con la informática era consecuencia del mayor empleo del proceso de datos en las economías y burocracias de los distintos países y que por ello se había difundido la comisión de actos delictivos.

Además, la injerencia transnacional en los sistemas de proceso de datos de otros países, había traído la atención de todo el mundo. Por tal motivo, si bien el problema principal - hasta ese entonces era la reproducción y la difusión no autorizada de programas informáticos y el uso indebido de los cajeros automáticos, no se habían difundido otras formas de *delitos informáticos*, por lo que era necesario adoptar medidas preventivas para evitar su aumento.

En general, se supuso que habría un gran número de casos de *delitos informáticos* no registrados.

Por todo ello, en vista de que los *delitos informáticos* eran un fenómeno nuevo, y debido a la ausencia de medidas que pudieran contrarrestarlos, se consideró que el uso deshonesto de las computadoras podría tener consecuencias desastrosas. A este respecto, el Congreso recomendó que se establecieran normas y directrices sobre la seguridad de las computadoras a fin de ayudar a la comunidad internacional a hacer frente a estas formas de delincuencia.

Partiendo del estudio comparativo de las medidas que se han adoptado a nivel internacional para atender esta problemática, deben señalarse los problemas que enfrenta la cooperación internacional en la esfera del *delito informático* y el derecho penal, a saber: la falta de consenso sobre lo que son los *delitos informáticos*, falta de definición jurídica de la conducta delictiva, falta de conocimientos técnicos por parte de quienes hacen cumplir la ley, dificultades de carácter procesal, falta de harmonización para investigaciones nacionales de *delitos informáticos*. Adicionalmente, la ausencia de la equiparación de estos delitos en los tratados internacionales de extradición.

Teniendo presente esa situación, consideramos que es indispensable resaltar que las soluciones puramente nacionales serán insuficientes frente a la dimensión internacional que caracteriza este problema. En consecuencia, es necesario que para solucionar los problemas derivados del incremento del uso de la informática, se desarrolle un régimen jurídico internacional donde se establezcan las normas que garanticen su compatibilidad y aplicación adecuada. Durante la elaboración de dicho régimen, se deberán de considerar los diferentes niveles de desarrollo tecnológico que caracterizan a los miembros de la comunidad internacional.

En otro orden de ideas, debe mencionarse que la *Asociación Internacional de Derecho Penal* durante un coloquio celebrado en Wurzburgo en 1992, adoptó

diversas recomendaciones respecto a los *delitos informáticos*. Estas recomendaciones contemplaban que en la medida en que el derecho penal tradicional no sea suficiente, deberá promoverse la modificación de la definición de los delitos existentes o la creación de otros nuevos, si no basta con la adopción de otras medidas (principio de subsidiaridad). Además, las nuevas disposiciones deberán ser precisas, claras y con la finalidad de evitar una excesiva tipificación deberá tenerse en cuenta hasta que punto el derecho penal se extiende a esferas afines con un criterio importante para ello como es el delimitar la responsabilidad penal con objeto de que éstos queden circunscritos primordialmente a los actos deliberados.

Considerando el valor de los bienes intangibles de la informática y las posibilidades delictivas que puede entrañar el adelanto tecnológico, se recomendó que los Estados consideraran de conformidad con sus tradiciones jurídicas y su cultura y con referencia a la aplicabilidad de su legislación vigente, la tipificación como delito punible de la conducta descrita en la "lista facultativa", especialmente la alteración de datos de computadora y el espionaje informático; así como que por lo que se refiere al delito de acceso no autorizado precisar más al respecto en virtud de los adelantos de la tecnología de la información y de la evolución del concepto de delincuencia.

Además, se señala que el tráfico con contraseñas informáticas obtenidas por medios inapropiados, la distribución de virus o de programas similares deben ser considerados también como susceptibles de penalización.

3.4 PARTICIPACIÓN NACIONAL SOBRE EL PROBLEMA INFORMATICO-JURÍDICO ACTUAL

El Instituto Nacional de Estadística, Geografía e Informática, en coordinación con la H. Cámara de Diputados tiene una participación en el análisis nacional sobre Derecho e Informática, con la finalidad de recopilar opiniones, propuestas y experiencias en torno al marco jurídico administrativo relacionado con la informática.

Este análisis se realizó en el marco del Programa de Desarrollo Informático en el cual, dentro de sus múltiples objetivos, señala el de contar con disposiciones jurídicas relativas a la informática que aseguren las condiciones requeridas para su mejor aprovechamiento.

Para la participación de este problema, se llevarón a cabo cinco reuniones en diferentes entidades del país, donde se analizarón y discutieron diversos temas con la finalidad de revisar el marco jurídico inherente a la informática. Asistieron al Foro alrededor de 620 representantes de los sectores público, privado, académico, empresarial y de investigación.

La primera de ellas se llevó a cabo en Veracruz, donde se abordaron aspectos en torno a la confidencialidad de la información personal almacenada en bases de datos públicos y privados, así como a la necesidad de brindar protección jurídica de los datos de carácter estratégico o confidencial producidos por los sectores público y privado.([43])

---

[43] Primer Congreso Nacional de Delitos Cibernéticos. México. 2000.

En este análisis, los comentarios se basaron en los siguientes puntos: propiedad de la información y derechos tanto del sujeto como del poseedor de los datos; responsabilidad por daños causados por mal uso de la información; derecho a que se preserve la confidencialidad de la información tanto de la que por ley es proporcionada al gobierno como de la que reciban los particulares; y, por último, acceso a la información propia almacenada en bases de datos y derecho a su revisión.

En la ciudad de Guadalajara, los temas analizados fuerón el de la tipificación de delitos cometidos con el uso de herramientas informáticas y, el valor probatorio del documento electrónico en procesos administrativos y judiciales.

Aquí los comentarios fuerón en relación con los siguientes aspectos: actividades informáticas que pueden considerarse como conductas delictivas y su definición; responsabilidad del uso de los datos confidenciales y personales tanto del prestador de servicio como del usuario; elementos que deben considerarse para determinar la responsabilidad de las personas autorizadas para administrar bases de datos; necesidad de definir el ámbito de aplicación del derecho informático; posibilidad de reconocimiento del documento electrónico como medio de prueba; y los requisitos que debe tener un sistema para que su bitácora sea reconocida legalmente. Asimismo, se presentó una propuesta de iniciativa de ley en la que se contemplan aspectos relacionados con las conductas que no están claramente tipificadas en el Código Penal vigente.

Posteriormente, en Monterrey se analizarón temas relacionados con la protección de los derechos de autor para desarrolladores de programas, así como de la información contenida en medios magnéticos y distribuida a través de redes de datos públicos, además de la protección de derechos de propiedad industrial.

En este evento resaltaron aspectos en torno a la importancia del procedimiento de registro de programas de cómputo; titularidad de derechos de los desarrollos que se realizan en empresas o instituciones por los trabajadores que intervienen en ellos; responsabilidad de los empleados que hacen uso de programas de cómputo ilegal en la empresa o institución en la que laboran; definición de términos jurídicos y técnicos para la solución de conflictos derivados del uso ilegal de programas de cómputo; la posible clasificación y reubicación, en su caso, de los programas de cómputo para su protección en el contexto de la Ley de Propiedad Industrial; y definición de contratos de bienes y servicios informáticos.

Los mecanismos de fomento al desarrollo y uso de la informática, así como las condiciones adecuadas de competencia y servicio entre los proveedores, fueron los temas que se analizarón en Tijuana, Baja California.

Los comentarios fueron alrededor de: la competitividad de empresas en el mercado informático; apoyos para el desarrollo de proyectos informáticos y mecanismos de evaluación; mecanismos para promover y fomentar el desarrollo de empresas de bienes y servicios informáticos; instancias de evaluación y certificación de calidad de este tipo de empresas; situación de las empresas desarrolladoras de programas de cómputo en el marco de la Ley Federal de Competencia Económica; y, programas de estudio de la licenciatura en derecho que incluyan conceptos informáticos.([44])

Finalmente, en el Distrito Federal, se realizarón algunas aproximaciones para análizar las condiciones para la prestación de los servicios telemáticos públicos y

---

[44] Articulo del Dr. Carlos M. Jarque. Presidente del INEGI. en el Foro de Consulta sobre Derecho e Informática. en el Boletin de Politica Informática. No. 7. año XIX. 1996.

privados, y el acceso universal a la información y a la infraestructura tecnológica. Para ello, se emitieron diversos comentarios en relación con el acceso a la información; utilidad y aplicación de la informática; regulación jurídica para propiciar el desarrollo informático; y sobre los derechos y responsabilidades de desarrolladores de programas para computadora.

Como resultado de estos cinco eventos que conformaron el Foro de Consulta sobre Derecho e Informática, se recibieron propuestas para líneas de acción inmediatas que permitirán revisar el marco jurídico-informatico. Entre ellas, destacan las siguientes:

- Realizar un estudio de derecho comparado y promover que exista congruencia de la legislación nacional con tratados internacionales de los que México forma parte.
- Promover la emisión de disposiciones que agilicen los procesos jurídicos y precisar el proceso para deslindar responsabilidades en caso de que se violen los derechos atórales protegidos por la ley.
- Protección de los derechos de propiedad intelectual e industrial para estimular la actividad creadora e instrumentar mecanismos técnicos y legales que propicien una protección más efectiva para minimizar el uso ilegal de programas para computadora.
- Definir los términos jurídicos que deben considerarse para su aplicación en litigios derivados de la violación a los derechos autorales o de algún ilícito cometido con el uso de esta tecnología.

- Establecer un modelo de "Derecho Informático" que contemple simultáneamente componentes jurídicos, educacionales y administrativos.

- Presentar propuestas de iniciativa de ley que contemplen aspectos relacionados con las conductas que no están claramente tipificadas en el Código Penal vigente y disposiciones complementarias.

- Tipificación del delito informático o electrónico como modalidad de los ya existentes a partir de la identificación y definición de sus características.

- Educar a las personas respecto a las consecuencias del mal uso de las tecnologías de información y promover la cultura en las universidades para apoyar la aplicación de las leyes.

- Que el gobierno fomente el mercado informático mediante la presentación de sus necesidades a la industria, licitando soluciones que posteriormente podrían ser utilizadas en el sector privado con sus correspondientes utilidades y creación de nuevas fuentes de trabajo.

- Ampliar conceptos en la ley que regula los procesos de adquisiciones para que sustenten la compra de soluciones más que de bienes informáticos.

- Promover la certificación de la calidad de empresas proveedoras de bienes y servicios informáticos y definir instancias que la validen.

- Promover mecanismos que regulen el comercio electrónico para que tenga mayor seguridad en las transacciones.

Tipificación de los delitos cometidos con el uso de herramientas informáticas que lesionan patrimonios y derechos de personas físicas y morales (sabotaje, fraude,

espionaje, etc.) y valor probatorio del documento electrónico en procesos administrativos y judiciales.

El manejo de la información dentro de las organizaciones es esencial para sus operaciones, esta información es resultado de la labor de la institución para recabarla, clasificarla, almacenarla y procesar mas información, esta situación convierte a la información en un recurso invaluable ya que la pérdida de la misma, la fuga y su caída en manos de la competencia o de enemigos puede ocasionar daños, pérdida de mercado o recursos capitalizables, prestigio y aún llevar a una empresa a la quiebra o pérdida de la credibilidad de las políticas de la administración pública.

Es por eso que se convierte en imprescindible el normar y legislar en las empresas y los organismos públicos sobre la tipificación de delitos informáticos.
Los fraudes electrónicos, el robo de información, la cada vez mayor participación de individuos sin profesionalismo y ética que no manejan de manera prudente y segura la información y que generan además código nocivo que afecta por igual a ambientes de cómputo y redes de comunicaciones con daño a los datos, también debe ser tipificado como delito.

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

La presente propuesta no es una posición personal del suscrito, es una recopilación de políticas que cubren los tópicos del tema y se presentan como una aportación que puede o no reflejar la opinión de otras personas que laboran dentro del área de seguridad informática.

3.5 ANÁLISIS LEGISLATIVO

Sobre el particular, y por considerar de interés el contenido de la exposición de motivos cuando esta ley se presentó ante la Cámara de Diputados, a continuación se presentan algunos comentarios pertinentes respecto a los elementos que deben contemplarse en la atención a la problemática de los derechos de autor en nuestro pais.

De esta forma, cuando se inició la iniciativa correspondiente, se dijo que la importancia de pronunciarse al respecto era que con dicha iniciativa se atendia la complejidad que el tema de los derechos autorales había presentado en los últimos tiempos lo cuál exigía una reforma con objeto de aclarar las conductas que podían tipificarse como delitos y determinar las sanciones que resultaran más efectivas para evitar su comisión.

Además, se consideró que debido a que en la iniciativa no se trataban tipos penales de delito se presentaba también una iniciativa de Decreto de Reforma al Código Penal para el Distrito Federal en materia de Fuero Federal, proponiendo la adición de un título Vigésimo Sexto denominado *"De los delitos en materia de derechos de autor"*([15]).

Al respecto, se consideró conveniente la inclusión de la materia en el ordenamiento materialmente punitivo, lo que por un lado habría de traducirse en un factor de impacto superior para inhibir las conductas delictivas y por otro en

[15] Exposición de motivos de la Comisión de Justicia de la Cámara de Diputados Doc.223/LVI/97 (II. P.O. Año III) DICT. que contiene el proyecto de decreto por el que se reforman la fracción III del artículo 231 de la Ley Federal del Derecho de Autor así como la fracción III del artículo 424 del Código Penal para el Distrito Federal en Materia del Fuero Común y para toda la República en Materia del Fuero Federal.

un instrumento más adecuado para la procuración y la administración de justicia, al poderse disponer en la investigación de los delitos y en su resolución, del instrumento general que orienta ambas funciones públicas.

Si bien pudiera pensarse que la inclusión de las sanciones a la fabricación de programas de virus en el Código Penal lleva implícito el reconocimiento de un *delito informático* debe tenerse presente que los delitos a regular en este título son en materia de derecho de autor, en el que el bien jurídico a tutelar es la propiedad intelectual, lo que limita su aplicación debido a que en los *delitos informáticos* el bien jurídico a tutelar serían por ejemplo el de la intimidad, patrimonio, etcétera.

La redacción de estas fracciones tratan de evitar la llamada piratería de programas en el área del comercio, permite la regulación administrativa de este tipo de conducta, como una posibilidad de agotar la vía administrativa antes de acudir a la penal, al igual que las infracciones contempladas para los programas de virus.

Además, la regulación de esta conducta se encuentra reforzada por la remisión que hace la Ley de Derecho de Autor en su artículo 215 al Título Vigésimo Sexto del Código Penal citado, donde se sanciona con multa de 300 a 3 mil días o pena de prisión de seis meses hasta seis años al que incurra en este tipo de delitos. Sin embargo, la regulación existente no ha llegado a contemplar el delito informático

como tal, sino que se ha concretado a la protección de los derechos autorales y de propiedad industrial, principalmente. ([46])

Tal y como hemos sostenido, México no está exento de formar parte de los países que se enfrentan a la proliferación de estas conductas ilícitas. Recientemente, la prensa publicó una nota en la que informaba sobre las pérdidas anuales que sufren las compañías fabricantes de programas informáticos, las que se remontaban a un valor de mil millones de dólares por concepto de piratería de estos programas.

Asimismo, consideramos que la protección a este tipo de bases de datos es necesaria en virtud de que la información contenida en ellas, puede contener datos de carácter sensible, como son los de las creencias religiosas o la filiación política. Adicionalmente pueden ser susceptibles de chantaje, los clientes de determinadas instituciones de créditos que posean grandes sumas de dinero, en fin, la regulación de la protección de la intimidad personal.

Por lo anterior, el análisis de éstos artículos corrobora la posición que hemos sostenido respecto a que en las conductas ilícitas relacionadas con la informáticas el bien jurídico a tutelar no es únicamente la propiedad intelectual sino la intimidad por lo que éstos artículos no debería formar parte de una Ley de derechos de autor sino de una legislación especial como el código penal tal y como se ha hecho en otros países.

En este entendido, consideramos que por la gravedad de la conducta ilícita en sí, y las implicaciones que traería aparejadas, justifica su regulación penal.

---

[46] Exposición de motivos de la Comisión de Justicia de la Cámara de Diputados Doc. 184/LVI/96 (I. P.O. Año III) DICT. durante el análisis de la Ley Federal de Derecho de Autor.

3.6 PAPEL QUE JUEGA EL ESTADO EN EL PROBLEMA INFORMATICO JURÍDICO DE LA ACTUALIDAD

- La posición del INEGI acerca del negocio de las PC es que requiere de creatividad y necesita un esfuerzo conjunto para educar a la comunidad virtual. A pesar de la realización reciente del Foro de Consulta sobre Derecho e Informática y los diversos trabajos en la Cámara de Diputados, falta mucho por hacer y se requiere una propuesta que satisfaga la realidad del país.

- El gobierno juega un papel importante en la creación de contenidos informativos nacionales y estadísticos que estén disponibles al público vía Internet. Se está fomentando una política de desarrollo del Internet a través de estrategias de acceso a la masa estudiantil en bibliotecas y gobiernos estatales, los cuales son esfuerzos menores que deben sumarse a las alternativas privadas (cafeterías, librerías y diversos lugares con terminales de acceso).

- La Secretaría de Gobernación tiene como función la de dar a conocer el servicio de información y publicarlo en el Diario Oficial de la Federación, órgano del Gobierno Constitucional de los Estados Unidos Mexicanos, cuyo objetivo es la difusión de las leyes y la normatividad en general, el cual ya está disponible vía Internet. Asimismo, se conserva el acervo de la historia jurídica del país en medios electrónicos y se pretende ponerlos a disposición del público en general.

- El Plan Nacional de Desarrollo menciona la promoción de servicios a través del Internet, en programas del INEGI.([47])

- La Secretaría de Contraloría y Desarrollo Administrativo actualmente norma aspectos de desarrollo y aprovechamiento de los servicios gubernamentales a través del Internet y se trabaja en el proyecto del Sistema Electrónico de Contrataciones Gubernamentales (COMPRANET). Lo anterior dará lugar a un mecanismo ágil y transparente de información y de rendición de cuentas a la ciudadanía a través de este mismo medio, originando una real contraloría social. Se requiere de un marco legal que fomente este desarrollo y se requiere otorgar valor jurídico generalizado a los documentos informáticos. Se pretende que a través del Internet se resuelvan necesidades (trámites gubernamentales, traslados de información sin papel, etc.), estableciendo oficinas electrónicas gubernamentales. De igual manera, se requiere un esquema de seguridad para dar validez a las firmas electrónicas, así como la creación de software de seguridad adaptado a nuestro país, dentro de un marco legal actualizado.

- Se está desarrollando un sistema de declaraciones patrimoniales transparente en mandos medios y superiores, con el fin de agilizar este trámite, ahorrando tiempo y recursos.

[47] Artículo publicado por el plan nacional de desarrollo (INEGI), sobre el derecho y la informática 1995-2000.

3.7 IMPACTO DE LOS DELITOS INFORMÁTICOS

Impacto a Nivel General

En los años recientes las redes de computadoras han crecido de manera asombrosa. Hoy en día, el número de usuarios que se comunican, hacen sus compras, pagan sus cuentas, realizan negocios y hasta consultan con sus médicos *online* supera los 200 millones, comparado con 26 millones en 1995.

A medida que se va ampliando la Internet, asimismo va aumentando el uso indebido de la misma. Los denominados delincuentes cibernéticos se pasean a su aire por el mundo virtual, incurriendo en delitos tales como el acceso sin autorización o "piratería informática", el fraude, el sabotaje informático, la trata de niños con fines pornográficos y el acecho.([48])

Los delincuentes de la informática son tan diversos como sus delitos; puede tratarse de estudiantes, terroristas o figuras del crimen organizado. Estos delincuentes pueden pasar desapercibidos a través de las fronteras, ocultarse tras incontables "enlaces" o simplemente desvanecerse sin dejar ningún documento de rastro. Pueden despachar directamente las comunicaciones o esconder pruebas delictivas en "paraísos informáticos" - o sea, en países que carecen de leyes o experiencia para seguirles la pista.
Según datos recientes del Servicio Secreto de los Estados Unidos, se calcula que los consumidores pierden unos 500 millones de dólares al año debido a los

[48] TELLEZ Valdés, Julio Delincuencia automatizada: los virus informáticos y el terrorismo por computadora. Tomado del libro Estudios Jurídicos en memoria de Jorge Barrera Graf. Ed. Porrúa. México. D.F., 1993. p446.

piratas que les roban de las cuentas *online* sus números de tarjeta de crédito y de llamadas. Dichos números se pueden vender por jugosas sumas de dinero a falsificadores que utilizan programas especiales para codificarlos en bandas magnéticas de tarjetas bancarias y de crédito, señala el Manual de la ONU.

Otros delincuentes de la informática pueden sabotear las computadoras para ganarle ventaja económica a sus competidores o amenazar con daños a los sistemas con el fin de cometer extorsión. Los malhechores manipulan los datos o las operaciones, ya sea directamente o mediante los llamados "gusanos" o "virus", que pueden paralizar completamente los sistemas o borrar todos los datos del disco duro. Algunos virus dirigidos contra computadoras elegidas al azar; que originalmente pasaron de una computadora a otra por medio de disquetes "infectados"; también se están propagando últimamente por las redes, con frecuencia camuflados en mensajes electrónicos o en programas "descargados" de la red.

En 1990, se supo por primera vez en Europa de un caso en que se usó a un virus para sonsacar dinero, cuando la comunidad de investigación médica se vio amenazada con un virus que iría destruyendo datos paulatinamente si no se pagaba un rescate por la "cura".

Los delincuentes cibernéticos al acecho también usan el correo electrónico para enviar mensajes amenazantes especialmente a las mujeres. De acuerdo al libro de Barbara Jenson "Acecho cibernético: delito, represión y responsabilidad personal en el mundo *online*", publicado en 1996, se calcula que unas 200.000 personas acechan a alguien cada año.

Afirma la Sra. Jensón de los Estados Unidos que una norteamericana fué acechada durante varios años por una persona desconocida que usaba el correo electrónico para amenazar con asesinarla, violar a su hija y exhibir la dirección de su casa en la Internet para que todos la vieran.

Los delincuentes también han utilizado el correo electrónico y los "*chat rooms*" o salas de tertulia de la Internet para buscar presas vulnerables. Por ejemplo, los aficionados a la pedofilia se han ganado la confianza de niños *online* y luego concertado citas reales con ellos para explotarlos o secuestrarlos. El Departamento de Justicia de los Estados Unidos dice que se está registrando un incremento de la pedofilia por la Internet.

Además de las incursiones por las páginas particulares de la Red, los delincuentes pueden abrir sus propios sitios para estafar a los clientes o vender mercancías y servicios prohibidos, como armas, drogas, medicamentos sin receta ni regulación y pornografía.

La *CyberCop Holding Cell*, un servicio de quejas *online*, hace poco emitió una advertencia sobre un anuncio clasificado de servicio de automóviles que apareció en la Internet. Por un precio fijo de $399, el servicio publicaría una descripción del auto del cliente en una página de la Red y garantizaban que les devolverían el dinero si el vehículo no se vendía en un plazo de 90 días.

Informa *CyberCop* que varios autos que se habían anunciado en la página electrónica no se vendieron en ese plazo, pero los dueños no pudieron encontrar a ninguno de los autores del servicio clasificado para que les reembolsaran el dinero. Desde entonces, el sitio en la Red de este "servicio" ha sido clausurado.

Respecto al uso de computadoras, Simon Nora y Alain Minc, en su libro Informatización de la sociedad, dicen: "Ayer las posibilidades de la informática estaba delimitada, eran comerciales, industriales o militares. De aquí en adelante, al dispersarse en una infinidad de pequeñas maquinas y ocultarse tras una red de ramificaciones ilimitadas.([49])

Impacto a Nivel Social

La proliferación de los delitos informáticos a hecho que nuestra sociedad sea cada vez más escéptica a la utilización de tecnologías de la información, las cuales pueden ser de mucho beneficio para la sociedad en general. Este hecho puede obstaculizar el desarrollo de nuevas formas de hacer negocios, por ejemplo el uso electrónico puede verse afectado por la falta de apoyo de la sociedad en general.

También se observa el grado de especialización técnica que adquieren los delincuentes para cometer éste tipo de delitos, por lo que personas con conductas maliciosas cada vez más están ideando planes y proyectos para la realización de actos delictivos, tanto a nivel empresarial como a nivel global.

También se observa que las empresas que poseen activos informáticos importantes, son cada vez más celosas y exigentes en la contratación de personal para trabajar en éstas áreas, pudiendo afectar en forma positiva o negativa a la sociedad laboral de nuestros tiempos.

[49] Nora, Simon y MINC, Alain. Op. Cit. p50

Aquellas personas que no poseen los conocimientos informáticos básicos, son más vulnerables a ser victimas de un delito, que aquellos que si los poseen. En vista de lo anterior aquel porcentaje de personas que no conocen nada de informática (por lo general personas de escasos recursos económicos) pueden ser engañadas si en un momento dado poseen acceso a recursos tecnológicos y no han sido asesoradas adecuadamente para la utilización de tecnologías como la Internet, correo electrónico, etc.

La falta de cultura informática puede impedir de parte de la sociedad la lucha contra los delitos informáticos, por lo que el componente educacional es un factor clave en la minimización de esta problemática.

A raíz de la gran trascendencia que ha adquirido la información, algunos autores como R. Hartley, aseveran que esta puede ser medida de su función de su utilidad, así la cantidad de información será proporcional al número de alternativas que se disponga en un numero dado.([50])

Impacto en la Esfera Judicial

Captura de delincuentes cibernéticos

A medida que aumenta la delincuencia electrónica, numerosos países han promulgado leyes declarando ilegales nuevas prácticas como la piratería informática, o han actualizado leyes obsoletas para que delitos tradicionales, incluidos el fraude, el vandalismo o el sabotaje, se consideren ilegales en el mundo virtual.

[50] TÉLLEZ, Valdés Julio. Derecho Informatico. Op cit p 66

Singapur, por ejemplo, enmendó recientemente su Ley sobre el Uso Indebido de las Computadoras. Ahora son más severos los castigos impuestos a todo el que interfiera con las "computadoras protegidas" es decir, las que están conectadas con la seguridad nacional, la banca, las finanzas y los servicios públicos y de urgencia así como a los transgresores por entrada, modificación, uso o intercepción de material computadorizado sin autorización.

Hay países que cuentan con grupos especializados en seguir la pista a los delincuentes cibernéticos. Uno de los más antiguos es la Oficina de Investigaciones Especiales de la Fuerza Aérea de los Estados Unidos, creada en 1978. Otro es el de Investigadores de la Internet, de Australia, integrado por oficiales de la ley y peritos con avanzados conocimientos de informática. El grupo australiano recoge pruebas y las pasa a las agencias gubernamentales de represión pertinentes en el estado donde se originó el delito.

Pese a estos y otros esfuerzos, las autoridades aún afrentan graves problemas en materia de informática. El principal de ellos es la facilidad con que se traspasan las fronteras, por lo que la investigación, enjuiciamiento y condena de los transgresores se convierte en un dolor de cabeza jurisdiccional y jurídico. Además, una vez capturados, los oficiales tienen que escoger entre extraditarlos para que se les siga juicio en otro lugar o transferir las pruebas y a veces los testigos al lugar donde se cometieron los delitos.

En 1992, los piratas de un país europeo atacaron un centro de computadoras de California. La investigación policial se vio obstaculizada por la doble tipificación penal --la carencia de leyes similares en los dos países que prohibían ese comportamiento-- y esto impidió la cooperación oficial, según informa el

Departamento de Justicia de los Estados Unidos. Con el tiempo, la policía del país de los piratas se ofreció a ayudar, pero poco después la piratería terminó, se perdió el rastro y se cerró el caso.

Asimismo, en 1996 el Servicio de Investigación Penal y la Agencia Federal de Investigación (FBI) de los Estados Unidos le siguió la pista a otro pirata hasta un país sudamericano. El pirata informático estaba robando archivos de claves y alterando los registros en computadoras militares, universitarias y otros sistemas privados, muchos de los cuales contenían investigación sobre satélites, radiación e ingeniería energética.([51])

Por lo que respecta a México hay grandes lagunas por lo que se refiere a sus legislaciones y por tal motivo quedan impunes muchos de los delitos que son cometidos aquí mismo y por tal motivo dicha impunidad se desprende de la falta de denuncias por parte de la sociedad. Por tal motivo hay posibles violaciones de las leyes nacionales. Sin embargo, México no a firmado acuerdos de extradición por delitos de informática sino por delitos de carácter más tradicional.

Destrucción u ocultación de pruebas

Otro grave obstáculo al enjuiciamiento por delitos cibernéticos es el hecho de que los delincuentes pueden destruir fácilmente las pruebas cambiándolas, borrándolas o trasladándolas. Si los agentes del orden operan con más lentitud que los delincuentes, se pierde gran parte de las pruebas; o puede ser que los datos estén cifrados, una forma cada vez más popular de proteger tanto a los particulares como a las empresas en las redes de computadoras.

[51] http://www.onnet.es/04001002.htm

Tal vez la criptografía (arte de escribir en claves de modo que sea posible descifrarlo), estorbe en las investigaciones penales, pero los derechos humanos podrían ser vulnerados si los encargados de hacer cumplir la ley adquieren demasiado poder técnico. Las empresas electrónicas sostienen que el derecho a la intimidad es esencial para fomentar la confianza del consumidor en el mercado de la Internet, y los grupos defensores de los derechos humanos desean que se proteja el cúmulo de datos personales archivados actualmente en ficheros electrónicos.

Las empresas también recalcan que la información podría caer en malas manos, especialmente en países con problemas de corrupción, si los gobiernos tienen acceso a los mensajes en código. "Si los gobiernos tienen la clave para descifrar los mensajes en código, esto significa que personas no autorizadas --que no son del gobierno-- pueden obtenerlas y utilizarlas", dice el gerente general de una importante compañía norteamericana de ingeniería de seguridad.

Impacto en la Identificación de Delitos a Nivel Mundial.

Las dificultades que enfrentan las autoridades en todo el mundo ponen de manifiesto la necesidad apremiante de una cooperación mundial para modernizar las leyes nacionales, las técnicas de investigación, la asesoría jurídica y las leyes de extradición para poder alcanzar a los delincuentes. Ya se han iniciado algunos esfuerzos al respecto.

En el Manual de las Naciones Unidas de 1977 se insta a los Estados a que coordinen sus leyes y cooperen en la solución de ese problema. El Grupo de Trabajo Europeo sobre delitos en la tecnología de la informática ha publicado un

Manual sobre el delito por computadora, en el que se enumeran las leyes pertinentes en los diversos países y se exponen técnicas de investigación, al igual que las formas de buscar y guardar el material electrónico en condiciones de seguridad.

El Instituto Europeo de Investigación Antivirus colabora con las universidades, la industria y los medios de comunicación y con expertos técnicos en seguridad y asesores jurídicos de los gobiernos, agentes del orden y organizaciones encargadas de proteger la intimidad a fin de combatir los virus de las computadoras o "caballos de Troya". También se ocupa de luchar contra el fraude electrónico y la explotación de datos personales.

En 1997, los países del Grupo de los Ocho aprobaron una estrategia innovadora en la guerra contra el delito de "tecnología de punta". El Grupo acordó que estableceria modos de determinar rápidamente la proveniencia de los ataques por computadora e identificar a los piratas, usar enlaces por video para entrevistar a los testigos a través de las fronteras y ayudarse mutuamente con capacitación y equipo. También decidió que se uniría a las fuerzas de la industria con miras a crear instituciones para resguardar las tecnologías de computadoras, desarrollar sistemas de información para identificar casos de uso indebido de las redes, perseguir a los infractores y recabar pruebas.([52])

Un obstáculo mayor opuesto a la adopción de una estrategia del tipo Grupo de los Ocho a nivel internacional es que algunos países no tienen la experiencia técnica ni las leyes que permitirían a los agentes actuar con rapidez en la búsqueda de

[52] http://personales-ciudad.com.ar/reble/thaissdelitos informaticos.htm

pruebas en sitios electrónicos --antes de que se pierdan-- o transferirlas al lugar donde se esté enjuiciando a los infractores.

3.8 ESTADÍSTICAS SOBRE DELITOS INFORMÁTICOS.

Desde hace cinco años, en los Estados Unidos existe una institución que realiza un estudio anual sobre la Seguridad Informática y los crímenes cometidos a través de las computadoras.

Esta entidad es El Instituto de Seguridad de Computadoras (CSI), quien anunció recientemente los resultados de su quinto estudio anual denominado "Estudio de Seguridad y Delitos Informáticos" realizado a un total de 273 Instituciones principalmente grandes Corporaciones y Agencias del Gobierno.

Este Estudio de Seguridad y Delitos Informáticos es dirigido por CSI con la participación Agencia Federal de Investigación (FBI) de San Francisco, División de delitos informáticos. El objetivo de este esfuerzo es levantar el nivel de conocimiento de seguridad, así como ayudar a determinar el alcance de los Delitos Informáticos en los Estados Unidos de Norteamérica.

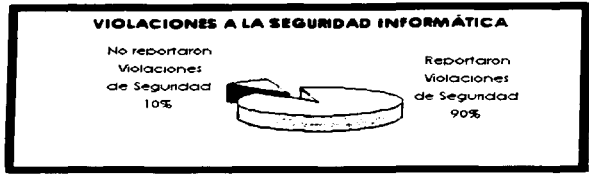
Entre lo más destacable del Estudio de Seguridad y Delitos Informáticos 2000 se puede incluir lo siguiente:

Violaciones a la seguridad informática.

Respuestas	PORCIENTC. (%)

No reportaron Violaciones de Seguridad 10%

90%



Reportar

Violaciones de Seguridad

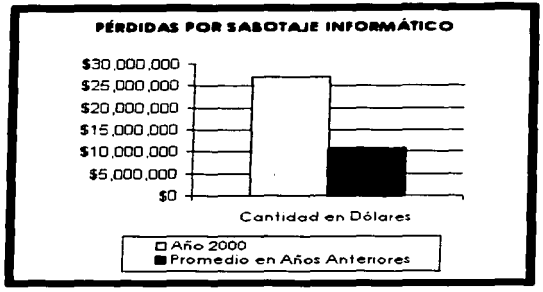
90% de los encuestados descubrió violaciones a la seguridad de las computadoras dentro de los últimos doce meses.

70% reportaron una variedad de serias violaciones de seguridad de las computadoras, y que el más común de estas violaciones son los virus de computadoras, robo de computadoras portátiles o abusos por parte de los empleados -- por ejemplo, robo de información, fraude financiero, penetración del sistema por intrusos y sabotaje de datos o redes.

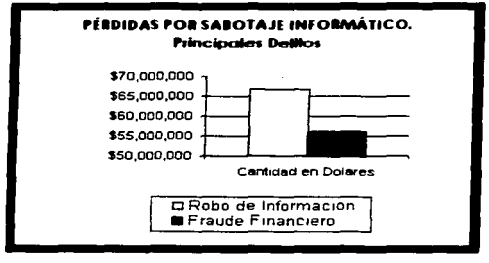
Pérdidas Financieras.

74% reconocieron pérdidas financieras debido a las violaciones de las computadoras.

Las pérdidas financieras ascendieron a $265,589,940 (el promedio total anual durante los últimos tres años era $120,240,180).



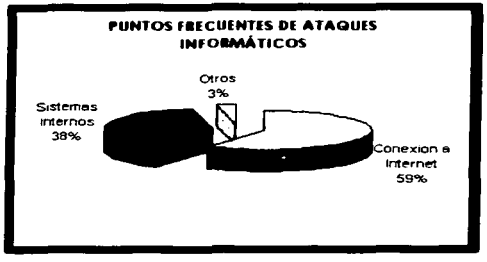
61 encuestados cuantificaron pérdidas debido al sabotaje de datos o redes para un total de $27,148,000. Las pérdidas financieras totales debido al sabotaje durante los años anteriores combinados ascendido a sólo $10,848,850.



Como en años anteriores, las pérdidas financieras más serias, ocurrieron a través de robo de información (66 encuestados reportaron $66,708,000) y el fraude financiero (53 encuestados informaron $55,996,000).

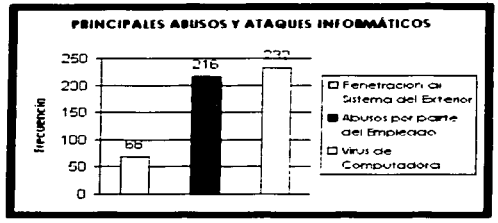
Los resultados del estudio ilustran que esa amenaza del crimen por computadoras a las grandes corporaciones y agencias del gobierno viene de ambos lados dentro y fuera de sus perímetros electrónicos, confirmando la tendencia en años anteriores.

Accesos no autorizados.



71% de los encuestados descubrieron acceso desautorizado por personas dentro de la empresa. Pero por tercer año consecutivo, la mayoría de encuestados (59%) mencionó su conexión de Internet como un punto frecuente de ataque, los que citaron sus sistemas interiores como un punto frecuente de ataque fué un 38%.

Basado en contestaciones de 643 practicantes de seguridad de computadoras en corporaciones americanas, agencias gubernamentales, instituciones financieras, instituciones médicas y universidades, los hallazgos del "Estudio de Seguridad y Delitos Informáticos 2000" confirman que la amenaza del crimen por computadoras y otras violaciones de seguridad de información continúan constantes y que el fraude financiero está ascendiendo.



Los encuestados detectaron una amplia gama de ataques y abusos. Aquí están algunos otros ejemplos:

- 25% de encuestados descubrieron penetración al sistema del exterior.
- 79% descubrieron el abuso del empleado por acceso de Internet (por ejemplo, transmitiendo pornografía o pirateó de software, o uso inapropiado de sistemas de correo electrónico).
- 85% descubrieron virus de computadoras.

Por segundo año, se realizaron una serie de preguntas acerca del comercio electrónico por Internet. Aquí están algunos de los resultados:

1. 93% de encuestados tienen sitios de WWW.
2. 43% maneja el comercio electrónico en sus sitios (en 1999, sólo era un 30%).
3. 19% experimentaron accesos no autorizados o inapropiados en los últimos doce meses.

4. 32% dijeron que ellos no sabían si hubo o no, acceso no autorizado o inapropiado.
5. 35% reconocieron haber tenido ataques, reportando de dos a cinco incidentes.
6. 19% reportaron diez o más incidentes.
7. 64% reconocieron ataques reportados por vandalismo de la Web.
8. 8% reportaron robo de información a través de transacciones.
9. 3% reportaron fraude financiero.

Conclusión sobre el estudio CSI:

Las tendencias que el estudio de CSI/FBI ha resaltado por años son alarmantes. Los "Cyber crímenes" y otros delitos de seguridad de información se han extendido y diversificado. El 90% de los encuestados reportaron ataques. Además, tales incidentes pueden producir serios daños. ([53])

Por tal motivo en México no existe una persecución de dichos delitos como se trabaja en otros países por lo mismo es necesario implantar y trabajar sobre los delitos informaticos que se manejan en México y así mismo implantar una serie de medidas penales que podría reducir este problema que nos rodea, no seria posible terminar o acabar con el problema en general peso se lograría una gran ventaja sobre los incidentes.

[53] Robo y Manipulación informática Articulo publicado por el instituto de seguridad de computadoras. Estados Unidos de Norte América año 2000.

3.9 EFECTOS POSITIVOS Y NEGATIVOS DE LA INFORMATICA EN LA ACTUALIDAD

A) EFECTOS POSITIVOS DE LA INFORMATICA

Dentro de las implicaciones positivas del uso de la computadora consideradas desde un punto de vista económico, se encuentran las siguientes:

a). AUMENTO EN LA PRODUCTIVIDAD.

La utilización de sistemas de computación en las compañías evita el desperdicio y mejora la eficiencia, lo cual da como resultado productos de mejor calidad y de precios mas bajos, así como un mejor servicio a los clientes. El uso de sistema de información, según la opinión de Nora y Minc, aportará un considerable incremento en la productividad, la cual podrá en mejores condiciones de competitividad y abrirá nuevos causes.([54])

La tendencia a la fabricación con computadora incrementa la productividad de manera significativa y el panorama resultante de éste incremento posibilitará que Un mayor número de personas obtenga un nivel de vida más alto, semanas laborales más cortas y más tiempo libre.

b). MEJOR SERVICIO.

El empleo de las computadoras en los negocios repercute mejor servicio a los clientes; por mencionar algunos:

[54] Nora, Simon y Minc, Alain Op cit p 19.

- Decremento en los precios de los productos, consecuencia de evitar el desperdicio y mejorar la eficiencia.

- Menos tiempo de espera en las oficinas de prestadores de servicios como venta de boletos de líneas aéreas, reservaciones de hoteles o renta de autos entre otros.

- Solución más rápida y precisa a las preguntas formuladas por personas a las que la empresa presta sus servicios.

c) NUEVAS OPORTUNIDADES DE TRABAJO.

Se han creado cientos de miles de nuevos empleos en áreas como la programación, la operación de computadoras y la administración de sistemas de información, donde la demanda actual de personas calificadas para hacer éstos trabajos es muy superior a la oferta.

Por lo general se dan cifras de las personas que han quedado desempleadas como resultado de la automatización, pero no de las que carecerían de trabajo de no haber llegado la nueva tecnología.

d). MAYOR SATISFACCION EN EL TRABAJO.

Se pueden resolver problemas sumamente complejos por medio de las computadoras en tiempos relativamente breves o, también, dejarle al procesamiento de la máquina las tareas peligrosas, repetitivas o aburridas,

liberando así a la mente humana de tareas desagradables y de ésta forma el hombre dispondrá de tiempo libre para concentrarse en aspectos más atractivos de su propia existencia.

B) EFECTOS NEGATIVOS DE LA INFORMÁTICA

1.DESEMPLEO. Debido al mejoramiento de la productividad lograda gracias al uso de las computadoras habrá un considerable despido de mano de obra. Así mismo, a mayor eficiencia que se logre por su uso, puede resultar Una mayor supresión de la actividad de algunos trabajadores, es decir, las computadoras reemplazan a las personas, por lo que el trabajador vive con el temor de perder el empleo o sufrir sino Una reducción en el salario, si en la periodicidad del aumento de éste por méritos personales. Cuando el empleado cree que ha perdido el control sobre su trabajo, el resultado puede ser, aparte de un decremento en su rendimiento, Un sabotaje a la computadora o al sistema.

2.DESCALIFICACION. El uso generalizado de la computadora acarrea la descalificación de muchos trabajos que hasta ahora eran ejecutados por una mano de obra muy experta, restándole importancia a sus actividades y convirtiendo al trabajador especializado en un simple supervisor, lo cual probablemente signifique la desaparición de su oficio y de su gremio.

3. INADAPTACIÓN. Mientras la computadora eleva la productividad también incrementa la tensión nerviosa del empleado creando el aburrimiento en el trabajo, minando la lealtad a la empresa y disminuyendo su producción, lo que provoca que éste sienta que sus capacidades y méritos se vean opacados por ésta máquina y empiece a considerarse insignificante y agobiado.

La informatización y trivialidad de las pocas tareas de carácter impersonal y repetitivo que todavia realice el empleado no preparado en la automatización. vendrán acompañadas de nuevos aspectos penosos como el tedio y la monotonia, lo cual le acarreará al trabajador problemas más psicológicos que fisicos al tener que vivir el trabajo de una manera distinta a la que ha estado habituado.

4. DESPLAZAMIENTO. El uso de robots controlados por computadoras está acelerando el desplazamiento, pues éstos realizan sin quejarse labores monótonas, sucias y peligrosas. Los problemas que se derivan de los puestos afectados por el desplazamiento son graves, pues se tiende a eliminar a los trabajadores de mayor edad o a reubicarlos en puestos para los que no están preparados; la falta de experiencia y conocimiento sobre los mismos, les ocasiona una pérdida de confianza en si mismos, aparte del temor a la posibilidad de no tener capacidad para adquirir las habilidades necesarias para desempeñar su nueva actividad, reduciendo asi su autoestima, pues empiezan a sentirse no sólo viejos sino también inútiles.

Sobre los efectos que la automatización impone sobre el empleo, Nora y Mmc expresan: "La informática permite y acelera el advenimiento de una sociedad de altisima productividad: menos trabajo para una mayor eficacia y unos puestos de trabajo muy diferentes de los que impone la vida industrial. Esta mutación ha empezado ya: fuerte disminución de la mano de obra en los sectores primarios y secundarios, alza de los servicios y sobre todo, multiplicación de las actitudes en las que la información es la materia prima. La acompañarán un cambio en la estructura de las organizaciones y una mudanza de las actitudes hacia el trabajo"([55]).

[55]NORA. Simon y MINC. Alain. Op. Cit. Pp. 175 y 176.

CAPITULO IV

LA LEGISLACIÓN MEXICANA Y SU COMPARACIÓN EN LA ACTUALIDAD CON EL DERECHO COMPARADO EN PAÍSES DE AMÉRICA Y EUROPA.

Se ha dicho que algunos casos de abusos relacionados con la informática deben ser combatidos con medidas jurídico-penales. No obstante, para aprehender ciertos comportamientos merecedores de pena con los medios del Derecho penal tradicional, existen, al menos en parte, relevantes dificultades. Estas proceden en buena medida, de la prohibición jurídico-penal de analogía y en ocasiones, son insuperables por la vía jurisprudencial. De ello surge la necesidad de adoptar medidas legislativas. En los Estados industriales de Occidente existe un amplio consenso sobre estas valoraciones, que se refleja en las reformas legales de los últimos diez años.

Pocos son los países que disponen de una legislación adecuada para enfrentarse con el problema sobre el particular, sin embargo con objeto de que se tomen en cuenta las medidas adoptadas por ciertos países, a continuación se presenta los siguientes casos particulares:

4..1 ALEMANIA

En Alemania para hacer frente a la delincuencia relacionada con la informática y con efectos a partir del 1 de agosto de 1986, se adoptó la Segunda Ley contra la Criminalidad Económica del 15 de mayo de 1986 en la que se contemplan los siguientes delitos:

Espionaje de datos (202 a);
Estafa informática (263 a);

Falsificación de datos probatorios (269) junto a modificaciones complementarias del resto de falsedades documentales como el engaño en el tráfico jurídico mediante la elaboración de datos, falsedad ideológica, uso de documentos falsos (270, 271, 273);

Alteración de datos (303 a) es ilícito cancelar, inutilizar o alterar datos inclusive la tentativa es punible;

Sabotaje informático (303 b), destrucción de elaboración de datos de especial significado por medio de destrucción, deterioro, inutilización, eliminación o alteración de un sistema de datos. También es punible la tentativa;

Utilización abusiva de cheques o tarjetas de crédito (266 b).

Por lo que se refiere a la estafa informática, la formulación de un nuevo tipo penal tuvo como dificultad principal el hallar un equivalente análogo al triple requisito de acción engañosa, acusación del error y disposición patrimonial, en el engaño del computador, así como en garantizar las posibilidades de control de la nueva expresión legal, quedando en la redacción que el perjuicio patrimonial que se comete consiste en influir en el resultado de una elaboración de datos por medio de una realización incorrecta del programa, a través de la utilización de datos incorrectos o incompletos, mediante la utilización no autorizada de datos, o a través de una intervención ilícita.

Sobre el particular, cabe mencionar que esta solución en forma parcialmente abreviada fué también adoptada en los Países Escandinavos y en Austria.

En opinión de estudiosos de la materia, el legislador alemán ha introducido un número relativamente alto de nuevos preceptos penales, pero no ha llegado tan lejos como los Estados Unidos. De esta forma, dicen que no sólo ha renunciado a tipificar la mera penetración no autorizada en sistemas ajenos de computadoras, sino que tampoco ha castigado el uso no autorizado de equipos de procesos de datos, aunque tenga lugar de forma cualificada.

En el caso de Alemania, se ha señalado que a la hora de introducir nuevos preceptos penales para la represión de la llamada criminalidad informática el gobierno tuvo que reflexionar acerca de dónde radicaban las verdaderas dificultades para la aplicación del Derecho penal tradicional a comportamientos dañosos en los que desempeña un papel esencial la introducción del proceso electrónico de datos, así como acerca de qué bienes jurídicos merecedores de protección penal resultaban así lesionados.

Fué entonces cuando se comprobó que, por una parte, en la medida en que las instalaciones de tratamiento electrónico de datos son utilizadas para la comisión de hechos delictivos, en especial en el ámbito económico, pueden conferir a éstos una nueva dimensión, pero que en realidad tan sólo constituyen un nuevo *modus operandi*, que no ofrece problemas para la aplicación a determinados tipos.

Por otra parte, sin embargo, la protección fragmentaria de determinados bienes jurídicos ha puesto de relieve que éstos no pueden ser protegidos suficientemente por el Derecho vigente contra nuevas formas de agresión que pasan por la utilización abusiva de instalaciones informáticas.

En otro orden de ideas, las diversas formas de aparición de la criminalidad informática propician además, la aparición de nuevas lesiones de bienes jurídicos merecedoras de pena, en especial en la medida en que el objeto de la acción puedan ser datos almacenados o transmitidos o se trate del daño a sistema informáticos. El tipo de daños protege cosas corporales contra menoscabos de su sustancia o función de alteraciones de su forma de aparición.

4.2 ARGENTINA

En Argentina, aún no existe legislación especifica sobre los llamados ***delitos informáticos***. Sólo están protegidas las obras de bases de datos y de software, agregados a la lista de items contemplados por la Ley 11.723 de propiedad intelectual gracias al Decreto N° 165/94 del 8 de febrero de 1994.

En dicho Decreto se definen:

Obras de software: Las producciones que se ajusten a las siguientes definiciones:

1. Los diseños, tanto generales como detallados, del flujo lógico de los datos en un sistema de computación.

2. Los programas de computadoras, tanto en versión "fuente", principalmente destinada al lector humano, como en su versión "objeto", principalmente destinada a ser ejecutada por la computadora.

3. La documentación técnica, con fines tales como explicación, soporte o entrenamiento, para el desarrollo, uso o mantenimiento de software.

Obras de base de datos: Se las incluye en la categoría de "obras literarias", y el término define a las producciones "constituidas por un conjunto organizado de datos interrelacionados, compilado con miras a su almacenamiento, procesamiento y recuperación mediante técnicas y sistemas informáticos"([57]).

De acuerdo con los códigos vigentes, para que exista robo o hurto debe afectarse una cosa, entendiendo como cosas aquellos objetos materiales susceptibles de tener algún valor, la energía y las fueras naturales susceptibles de apropiación. **(Código Civil, Art. 2311).**

Asimismo, la situación legal ante daños infligidos a la información es problemática:

- El **artículo 1072** del Código Civil argentino declara *"el acto ilícito ejecutado a sabiendas y con intención de dañar la persona o los derechos del otro se llama, en este Código, delito"*, obligando a reparar los daños causados por tales delitos.

- En caso de probarse la existencia de delito de daño por destrucción de la cosa ajena, *"la indemnización consistirá en el pago de la cosa destruida; si la destrucción de la cosa fuera parcial, la indemnización consistirá en el pago de la diferencia de su valor y el valor primitivo"* **(Art. 1094).**

[57] TRAMITE PARLAMENTARIO No. 19 Ley Nacional de Informatica, Argentina. 1986. p 474

- Existe la posibilidad de reclamar indemnización cuando el hecho no pudiera ser considerado delictivo, en los casos en que *"alguien por su culpa o negligencia ocasiona un daño a otro"* **(Art. 1109).**

- Pero *"el hecho que no cause daño a la persona que lo sufre, sino por una falta imputable a ella, no impone responsabilidad alguna"* **(Art. 1111).**

- En todos los casos, el resarcimiento de daños consistirá en la reposición de las cosas a su estado anterior, excepto si fuera imposible, en cuyo caso la indemnización se fijará en dinero" **(Art. 1083).**

El mayor inconveniente es que no hay forma de determinar fehacientemente cuál era el estado anterior de los datos, puesto que la información en estado digital es fácilmente adulterable. Por otro lado, aunque fuera posible determinar el estado anterior, sería difícil determinar el valor que dicha información tenía, pues es sabido que el valor de la información es subjetivo, es decir, que depende de cada uno y del contexto.

Lo importante en este tema es determinar que por más que se aplique la sanción del artículo 72 de la ley 11723, la misma resulta insuficiente a efectos de proteger los programas de computación, los sistemas o la información en ellos contenidos de ciertas conductas delictivas tales como: el ingreso no autorizado, la violación de secretos, el espionaje, el uso indebido, el sabotaje, etc.

4.3 AUSTRIA.

Ley de reforma del Código Penal de 22 de diciembre de 1987.

Esta ley contempla los siguientes delitos:

Destrucción de datos (126). En este artículo se regulan no sólo los datos personales sino también los no personales y los programas.

Estafa informática (148). En este artículo se sanciona a aquellos que con dolo causen un perjuicio patrimonial a un tercero influyendo en el resultado de una elaboración de datos automática a través de la confección del programa, por la introducción, cancelación o alteración de datos por actuar sobre el curso del procesamiento de datos. Además contempla sanciones para quienes cometen este hecho utilizando su profesión.

4.4 CANADÁ

Este país, el texto adoptado en Abril de 1985 fué resultado de los trabajos de un Comité Especial reunido para estudiar "las infracciones relativas a las computadoras".

Con la voluntad manifiesta de respetar "el principio fundamental del Derecho penal según el cual la definición de las infracciones debe ser precisa y justa

de manera que permita una interpretación conveniente de las disposiciones legislativas e indique adecuadamente al publico las actividades que están precisamente prohibidas.([57]) el legislador canadiense creó dos nuevas infracciones:

1.El uso no autorizado de un sistema informático.

2. La modificación o destrucción no autorizada de datos informatizados.

Asi mismo, ha hecho evidente su preocupación por las medidas preventivas que se pueden aplicar. Una de las recomendaciones hechas por el Comité es que "los profesores de informática estén debidamente calificados en el ámbito de la ética en informática". Consideramos que con esta medida pretenden crear conciencia en el personal especializado en la materia en cuestión, pues normalmente incurren en el delito informático debido a la facilidad de su comisión y al uso de la máquina, factores que los orillan a minimizar el daño provocado a terceros.
El texto al que nos referimos al inicio de este punto nos remite a un nuevo artículo inserto en el Código Criminal, el 301.2, el cual en su primera parte menciona:

"Cualquiera que fraudulosamente y sin apariencia de derecho:

a) Obtenga cualquier servicio computarizado directa o indirectamente.

b) Por medio de un dispositivo electromagnético, acústico, mecánico o de

[57] VIVANTI. Michel. Droit de Informatique Paris. Edit. Lamy. S.A . 1986 . p 1029.

cualquier otro tipo, directa o indirectamente intercepte o haga interceptar toda función de un sistema de cómputo; o

c) Directa o indirectamente utilice o haga utilizar un sistema de cómputo con la intención de cometer una falta de las señaladas en las Fracciones (*a*) o (*b*) o una de las infracciones previstas en el Artículo 387 concernientes a los datos o a los sistemas de cómputo;

es culpable de un acto criminal y sujeto a una pena de privación de la libertad que no excederá de 10 años o es culpable de una infracción castigable sobre declaración sumaria de culpabilidad".

La parte Dos de este artículo se encarga de precisar las definiciones que son de gran importancia en la interpretación de los tipos penales alusivos tales como:

PROGRAMA DE COMPUTO: Significa datos que representan instrucciones o estados de cuenta que cuando son ejecutados en un sistema de cómputo, dan lugar a que éste realice una función.

SERVICIO DE COMPUTO: Incluye el procesamiento de datos y el almacenamiento o recuperación de los mismos.

SISTEMA DE COMPUTO: Significa un dispositivo o grupo de éstos que estén interconectados o relacionados, los cuales

(a) Contengan programas de cómputo u otros datos; y

(b) Conforme a los programas de cómputo:

1. Realicen lógica y control; y
2. Puedan realizar cualquier otra función.

El Articulo 387 a que se refiere el Inciso (c) de la Sección uno del Articulo 301.2, trata de proteger la esencia de los datos informatizados, haciendo acreedora a una pena no mayor de 10 años a la persona que:

(a) Destruya o altere los datos.

(b) Transforme los datos haciéndolos incomprensibles inútiles o ineficaces.

(c) Obstruya, interrumpa o interfiera con el uso legítimo de los datos; o

(d) Obstruya, interrumpa o interfiera con cualquier persona en el legítimo uso de los datos o niegue el acceso a éstos a toda persona que esté autorizada para ello.

En cuanto a las definiciones utilizadas en el Código Criminal de Canadá respecto a los delitos informáticos, estimamos que algunas de ellas no son las apropiadas debido a su falta de precisión, característica que el gobierno Canadiense considera fundamental en el Derecho Penal, como ya se dijo, para una interpretación conveniente de sus disposiciones.

Respecto a la forma en que este país está enfrentando el problema derivado del mal uso de las computadoras y de la información que éstas contienen, consideramos que aunque de manera concisa, está siendo substancioso y el hecho de que ya cuenten con una figura jurídico-penal que sancione estas conductas, ha sido benéfico pues su comisión ha disminuido.

4.5 CHILE

Chile fué el primer país latinoamericano en crear una **Ley contra delitos informáticos**, la cual entró en vigencia el 7 de junio de 1993.

Según esta ley, la destrucción o inutilización de los datos contenidos dentro de una computadora es castigada con penas desde un año y medio a cinco años de prisión. Asimismo, dentro de esas consideraciones se encuentran los virus.

Esta ley prevé en el Art. 1°, el tipo legal vigente de una conducta maliciosa tendiente a la destrucción o inutilización de un sistema de tratamiento de información o de sus partes componentes o que dicha conducta impida, obstaculice o modifique su funcionamiento. En tanto, el Art. 3° tipifica la conducta maliciosa que altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información.

4.6 ESPAÑA

España fué el primer país europeo en aplicar la técnica investigación de delitos en Internet. La intervención tuvo lugar en diciembre de 1996, a raíz de una denuncia por distribución no autorizada de programas, obras multimedia y bases de datos jurídicas a través de Internet. El mandamiento judicial recogió cada uno de los pasos necesarios para la interceptación de los mensajes de correo electrónico del presunto infractor y su grabación automática en el disco duro de un ordenador habilitado al efecto.

Los treinta días de la intervención telemática arrojaron pruebas concluyentes de la infracción, ya que, junto a los mensajes transferidos se hallaron catálogos, pedidos, órdenes de transferencias de fondos, *cracks* y los propios programas distribuidos ilícitamente.

En el ***Nuevo Código Penal de España***, el artículo 263 establece que el que causare daños en propiedad ajena. En tanto, el artículo 264-2) establece que se aplicará la pena de prisión de uno a tres años y multa a quien por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos.

El ***nuevo Código Penal de España*** sanciona en forma detallada esta categoría delictual (Violación de secretos/Espionaje/Divulgación), aplicando pena de prisión y multa, agravándolas cuando existe una intención dolosa y cuando el hecho es cometido por parte funcionarios públicos se penaliza con inhabilitación.

En materia de estafas electrónicas, el ***nuevo Código Penal de España***, en su artículo 248, solo tipifica las estafas con ánimo de lucro valiéndose de alguna manipulación informática, sin detallar las penas a aplicar en el caso de la comisión del delito.

4.7 ESTADOS UNIDOS DE NORTE AMÉRICA

Este pais adoptó en 1994 del **Acta Federal de Abuso Computacional (18 U.S.C. Sec.1030)** que modificó al Acta de Fraude y Abuso Computacional de 1986.

Con la finalidad de eliminar los argumentos hipertécnicos acerca de qué es y que no es un virus, un gusano, un caballo de Troya y en que difieren de los virus, la nueva acta proscribe la transmisión de un programa, información, códigos o comandos que causan daños a la computadora, a los sistemas informáticos, a las redes, información, datos o programas (18 U.S.C.: Sec. 1030 (a) (5) (A). La nueva ley es un adelanto porque está directamente en contra de los actos de transmisión de virus.

El Acta de 1994 diferencia el tratamiento a aquellos que de manera temeraria lanzan ataques de virus de aquellos que lo realizan con la intención de hacer estragos. Definiendo dos niveles para el tratamiento de quienes crean virus.

Para los que intencionalmente causan un daño por la transmisión de un virus, el castigo de hasta 10 años en prisión federal más una multa.

Para los que lo transmiten sólo de manera imprudencial la sanción fluctúa entre una multa y un año en prisión.

La nueva ley constituye un acercamiento más responsable al creciente problema de los virus informáticos, específicamente no definiendo a los virus sino

describiendo el acto para dar cabida en un futuro a la nueva era de ataques tecnológicos a los sistemas informáticos en cualquier forma en que se realicen. Diferenciando los niveles de delitos, la nueva ley da lugar a que se contemple qué se debe entender como acto delictivo.

Asimismo, en materia de estafas electrónicas, defraudaciones y otros actos dolosos relacionados con los dispositivos de acceso a sistemas informáticos, la legislación estadounidense sanciona con pena de prisión y multa, a la persona que defraude a otro mediante la utilización de una computadora o red informática.

4.8 FRANCIA

En enero de 1988, este país dictó la **Ley relativa al fraude informático**, la cual prevé penas de dos meses a dos años de prisión y multas de diez mil a cien mil francos por la intromisión fraudulenta que suprima o modifique datos.

Asimismo, esta ley establece en su artículo 462-3 una conducta intencional y a sabiendas de estar vulnerando los derechos de terceros que haya impedido o alterado el funcionamiento de un sistema de procesamiento automatizado de datos. Por su parte el artículo 462-4 también incluye en su tipo penal una conducta intencional y a sabiendas de estar vulnerando los derechos de terceros, en forma directa o indirecta, haya introducido datos en un sistema de procesamiento automatizado o haya suprimido o modificado los datos que éste contiene, o sus modos de procesamiento o de transmisión.

También la legislación francesa establece un tipo doloso y pena el mero acceso, agravando la pena cuando resultare la supresión o modificación de datos

contenidos en el sistema, o bien en la alteración del funcionamiento del sistema (sabotaje).

Por último, esta ley en su artículo 462-2, sanciona tanto el acceso al sistema como al que se mantenga en él y aumenta la pena correspondiente si de ese acceso resulta la supresión o modificación de los datos contenidos en el sistema o resulta la alteración del funcionamiento del sistema.

4.9 GRAN BRETAÑA

Debido a un caso de *hacking* en 1991, comenzó a regir en este país la ***Computer Misuse*** **Act** (Ley de Abusos Informáticos). Mediante esta ley el intento, exitoso o no, de alterar datos informáticos es penado con hasta cinco años de prisión o multas.

Esta ley tiene un apartado que especifica la modificación de datos sin autorización. Los virus están incluidos en esa categoría.

El liberar un virus tiene penas desde un mes a cinco años, dependiendo del daño que causen.

4.10 HOLANDA

El 1° de Marzo de 1993 entró en vigencia la **Ley de Delitos Informáticos**, en la cual se penaliza el *hacking*, el *preacking* (utilización de servicios de

telecomunicaciones evitando el pago total o parcial de dicho servicio), la ingeniería social (arte de convencer a la gente de entregar información que en circunstancias normales no entregaría), y la distribución de virus.

La distribución de virus está penada de distinta forma si se escaparon por error o si fuerón liberados para causar daño.

Si se demuestra que el virus se escapó por error, la pena no superará el mes de prisión; pero, si se comprueba que fuerón liberados con la intención de causar daño, la pena puede llegar hasta los cuatro años de prisión.

4.11 MÉXICO

Para el desarrollo de este tema se analizará la legislación que regula administrativa y penalmente las conductas ilícitas relacionadas con la informática, pero que, aún no contemplan en sí los delitos informáticos. En este entendido, consideramos pertinente recurrir a aquellos tratados internacionales de los que el Gobierno de México es parte en virtud de que el artículo 133 constitucional establece que todos los tratados celebrados por el Presidente de la República y aprobados por el Senado serán Ley Suprema de toda la Unión.

A. Tratado de Libre Comercio de América del Norte (TLC)

Este instrumento internacional firmado por el Gobierno de México, de los Estados Unidos y Canadá en 1993, contiene un apartado sobre propiedad

intelectual, a saber la 6a. parte capítulo XVII, en el que se contemplan los derechos de autor, patentes, otros derechos de propiedad intelectual y procedimientos de ejecución.

En términos generales, puede decirse que en ese apartado se establecen como parte de las obligaciones de los Estados signatarios en el área que se comenta que deberán protegerse los programas de cómputo como obras literarias y las bases de datos como compilaciones, además de que deberán conceder derechos de renta para los programas de cómputo.

De esta forma, debe mencionarse que los tres Estados Parte de este Tratado también contemplaron la defensa de los derechos de propiedad intelectual (artículo 1714) a fin de que su derecho interno contenga procedimientos de defensa de los derechos de propiedad intelectual que permitan la adopción de medidas eficaces contra cualquier acto que infrinja los derechos de propiedad intelectual comprendidos en el capítulo específico del tratado.

En este orden y con objeto de que sirva para demostrar un antecedente para la propuesta que se incluye en el presente trabajo, debe destacarse el contenido del párrafo uno del artículo 1717 titulado Procedimientos y Sanciones Penales en el que de forma expresa se contempla la figura de piratería de derechos de autor a escala comercial.

Por lo que se refiere a los anexos de este capítulo, anexo 1718.14, titulado defensa de la propiedad intelectual, se estableció que México haría su mayor esfuerzo por cumplir tan pronto como fuera posible con las obligaciones del artículo 1718 relativo a la defensa de los derechos de propiedad intelectual en la

frontera, haciéndolo en un plazo que no excedería a tres años a partir de la fecha de la firma del TLC.([58])

Asimismo, debe mencionarse que en el artículo 1711, relativo a los secretos industriales y de negocios sobre la provisión de medios legales para impedir que estos secretos, sean revelados, adquiridos o usados sin el consentimiento de la persona que legalmente tenga bajo su control la información.

Llama la atención que en su párrafo 2 habla sobre las condiciones requeridas para otorgar la protección de los secretos industriales y de negocios y una de ellas es que estos consten en medios electrónicos o magnéticos.

En México como en tantos otros países no existe una tipificación legal en una legislación especial de estos delitos informaticos sin embargo en otros países se ha logrado.

B. ESTADO DE SINALOA

CODIGO PENAL Y PROCEDIMIENTOS PENALES DE SINALOA

Ante la importancia que tiene que el Congreso Local del Estado de Sinaloa haya legislado sobre la materia de delitos informaticos, consideramos pertinente transcribir íntegramente el texto que aparece en el Código Penal Estatal.

Título Décimo

[58] Tratado de Libre Comercio (TLC) Parte 3. Diario Oficial de la Federación. Lunes 20 de diciembre de 1993.

"Delitos contra el patrimonio"

Capitulo V

Delito Informático.

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

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

II. Intercepte, interfiera, reciba, use, altere, dañe o destruya un soporte lógico o programa de computadora o los datos contenidos en la misma, en la base, sistema o red.

Al responsable de delito informático se le impondrá una pena de seis meses a dos años de prisión y de noventa a trescientos días multa. En el caso particular que nos ocupa cabe señalar que en Sinaloa se ha contemplado al delito informático como uno de los delitos contra el patrimonio, siendo este el bien jurídico tutelado.

Consideramos que se ubicó al *delito informático* bajo esta clasificación dada la naturaleza de los derechos que se transgreden con la comisión de estos ilícitos, pero a su vez, cabe destacar que los *delitos informáticos* van más allá de una simple violación a los derechos patrimoniales de las víctimas, ya que debido a las diferentes formas de comisión de éstos, no solamente se lesionan esos derechos.

CAPITULO V

PROPUESTAS Y CONSIDERACIONES FINALES

5.1 ANÁLISIS JURÍDICO SOCIAL DE LA INFORMÁTICA Y SUS REPERCUSIONES EN EL DERECHO PENAL MEXICANO.

Como se puede apreciar, los temas cubiertos a lo largo de todo este estudio abarcan un amplio espectro, como brindar seguridad jurídica a la sociedad en cuanto al uso de su información, tipificación de delitos cometidos con el uso de herramientas informáticas, uso y valor de documentos electrónicos en procesos administrativos y judiciales, protección de derechos de autor y de propiedad industrial, mecanismos de fomento al desarrollo y uso de la informática, y condiciones de acceso universal a la infraestructura tecnológica y a la información.

Así, la investigación aborda desde las garantías individuales para la protección de información y hasta los derechos de las personas para aprovechar los beneficios de la informática.

Como fué referido en el presente trabajo, la informática es interesante en su perspectiva metodológica, es estimulante en sus aspectos técnicos, y es fascinante en su dimensión científica. Sin embargo, su verdadera nobleza estriba en la contribución que ésta puede brindar para lograr un México mejor.
Y para que la informática logre cabalmente su potencial de elemento estratégico en el desarrollo de nuestro país, se debe contar con un marco jurídico completo y coherente, que dé certidumbre y confianza. Sin él, el avance estaría seriamente restringido.

Este análisis sobre Derecho e Informática se convoca a la participación del Congreso de la Unión, lo cual es evidencia del decidido apoyo y del compromiso,

en estas materias, de distinguidos representantes del Poder Legislativo. Por ello, en este Foro se nos presenta la gran oportunidad de que las inquietudes, opiniones y sugerencias vertidas, se puedan traducir en propuestas concretas para la adecuación y establecimiento de disposiciones jurídicas y administrativas pertinentes a esta tecnología.

Prácticamente los temas a tratarse en estas investigación son novedosos. Su análisis también se está programando o iniciando en otros países. En México, la convocatoria ha sido muy oportuna y la decidida participación de toda la sociedad nos permite investigar sobre la que se inicia.

Estoy seguro que sabremos aprovechar esta oportunidad para contribuir a que el país cuente, en corto plazo, con disposiciones jurídicas más adecuadas en esta materia.

Así como tambien de que a través de estos análisis profundos lograremos avanzar en la construcción de los cimientos jurídicos y de la infraestructura legal, que permitan aprovechar la informática en el logro de los más nobles propósitos nacionales. De cara al futuro, esta es sin duda una actividad fundamental para el progreso de nuestra patria.

5.2 DIFUSIÓN A LA SOCIEDAD EN GENERAL SOBRE EL PROBLEMA QUE NOS OCUPA

A pesar del silencio de las Ciencia jurídicas y Tecnología ante esta demanda por parte de la Comunidad Internet, se pretende establecer una Asociación de Internautas, para que una vez más, dado un paso adelante con la puesta en

funcionamiento de esta iniciativa y se pide la colaboración y apoyo de todos los agentes implicados en el sector para su desarrollo y difusión.

Por ese motivo; a lo largo de estos últimos años, los contenidos de esta propuesta se irán incrementando a medida que colaboradores y expertos nos vayan enviando nuevas propuestas formativas y dentro del campo de la seguridad.

Para lo consiguiente se puede ofrecer una línea de contacto permanente mediante correo electrónico, para solucionar dudas, recibir sugerencias, aportaciones y colaboraciones, y de esta manera recoger de forma inmediata la participación y la respuesta que la Comunidad Internet preste a esta iniciativa.

Será necesario que el Gobierno ponga en marcha un plan de seguridad informática para impulsar el desarrollo de Internet y su utilización frecuente.

La noción recoge que la iniciativa de seguridad contemple las acciones del Plan de Acción Informática del siglo XXI y las medidas necesarias, "siempre de acuerdo a las conclusiones de la Comisión de Redes Informáticas que se generen.

Así, la iniciativa gubernamental, que deberá ser desarrollada "a la mayor brevedad posible", contempla de manera especial las campañas de prevención y difusión de información a los usuarios sobre la protección frente a virus informáticos, así como el desarrollo permanente de detección y alerta.

También asume la puesta en marcha de campañas de difusión de información y desarrollo del marco regulador necesario para promover la confianza de los

ciudadanos en el uso de Internet, "previniendo posibles abusos informaticos en la Red".

Se ha pensado en campañas en T.V., radio y periódico para crear conciencia sobre el delito informático así mismo que pueda haber una posible solución al problema que nos rodea.

5.3 BENEFICIOS Y PERJUICIOS DEL PROBLEMA INFORMATICO-JURÍDICO

Se propone concretamente el que al legislar en materia de Derecho Informático, sienten las bases para hacer posible el fincamiento de responsabilidad penal de los administradores de Redes de Cómputo, así como de los dueños de la red operada.

Se propone crear el tipo penal de Responsabilidad de los Administradores de Redes de Cómputo, bajo las bases siguientes:

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

B.- Que actúen de manera negligente ante el descubrimiento del irrumpiendo de un *Hacker*, o ante la existencia de cuentas con derechos excesivos sobre determinados directorios de la red.

C.- Que perpetren ellos mismos el ilícito consistente en: apoderamiento, modificación, utilización o destrucción no autorizada por el autor o el titular del derecho sobre el archivo.

Se propone crear el tipo penal de la responsabilidad de el Propietario de la red de cómputo, bajo las bases siguientes:

A.- Que no contrate a personas debidamente capacitadas para desempeñarse como administradores de la red computacional.

B.- El no haber prevenido la comisión de ilícitos, a través de proporcionar oportunamente cursos de capacitación a su (s) Administrador (es) de red.

C.- El no proporcionar los recursos necesarios para adquirir los programas necesarios para la adecuada conservación de el sistema de red, así como de los archivos en ella contenidos.

5.4 INTERPOSICIÓN DE MEDIDAS PREVENTIVAS Y CORRECTIVAS

MEDIDAS PREVENTIVAS

Como medida preventiva de tipo social, se propone la educación de la población respecto a los usos y abusos que se pueden llevar a cabo con las computadoras y las consecuencias de cualquier acción con y contra éstas, educación que se debe impartir desde la primaria, pues los niños en edad

escolar ya tienen contacto con estas máquinas y están creciendo junto con el desarrollo de las computadoras, lo que les ofrece facilidades para su uso o abuso. La computadora es una herramienta muy poderosa y el poder debe estar siempre acompañado de responsabilidad.

considero que de nada sirve que las computadoras y la información confidencial que éstas almacenan estén supuestamente protegidas contra daño o penetración o contra la diseminación de dicha información ya sea de manera accidental o maliciosa, si continúan siendo falibles y al no existir tipificación expresa que sancione tal conducta antijurídica, por lo mismo, el que la comete queda impune de acuerdo al principio *"nulla poena sine lege"*, no hay pena sin ley.

Por lo tanto, ante la incapacidad para resguardar los sistemas de información, las medidas preventivas de tipo jurídico que por su carácter punitivo funcionarían como correctivas que se proponen, son las siguientes:

- La tipificación del delito como delito nuevo que es, ya que hasta la fecha se vienen aplicando por analogía, aunque la Constitución expresamente lo prohíbe, el robo o el fraude y esta nueva conducta antijurídica no se adecua cabalmente a dichas figuras.

- obligar a quien lo sufre a denunciar el delito, pues generalmente no se efectúa porque las compañías afectadas que en la mayoría de los casos son bancos o empresas financieras así como particulares temen que de divulgarse éstos, acarrearían su desprestigio y generarían la desconfianza de sus clientes.

- Para que la integración de los elementos del tipo del delito se efectúe eficazmente y el proceso correspondiente sea justo, es necesario que todas las personas implicadas en dichas tareas como los agentes del ministerio publico, jueces, abogados, etc., cuenten con los conocimientos elementales sobre el uso de la computadora y que en la realización de un peritaje jurídico - informático intervengan expertos en ambas materias.

De lo anteriormente expuesto, concluimos que para la prevención abuso informático, como lo hemos denominado, se requiere:

- Instruir al público acerca de los usos, abusos y consecuencias que se pueden realizar con las computadoras.

- Instalar dispositivos de seguridad efectivos para evitar la intrusión a las computadoras.

- Desarrollar medidas de seguridad proyectadas para detectar a los infractores de la ley.

- Promulgar leyes especificas a este caso y exigir su observancia.

MEDIDAS CORRECTIVAS

Si bien el grado de informatización en nuestro país es incipiente, son claras las tendencias a una mayor incorporación de las nuevas tecnologías y toda vez

que en México, al igual que en muchos paises no existe un tipo especifico que sancione las nuevas conductas delictivas, estamos seguros de que la única medida correctiva que se puede imponer a esta situación es precisamente su tipificación.

El Derecho se halla hoy en día en una instancia histórica en la que debe responder a los nuevos y complejos problemas que le plantea la amplitud y profundidad del avance tecnológico en general y de informática en especial, por lo tanto, para salvar los vacios normativos, se deben dictar medidas penales especialmente referidas a los delitos informáticos, medidas que sean lo suficientemente generales y flexibles para ser aplicadas a pesar la rápida evolución de la tecnología computacional.

Creemos que la inclusión en las Legislaciones Penal Mexicanas de una figura jurídica creada expresamente para este fin, seria de gran utilidad no sólo por su carácter correctivo, ya que de existir una sanción para quien incurra en su comisión, se evitaría caer en ella, funcionando de esta manera también como medida preventiva.

Cabe aclarar que la existencia de una ley que sancione esta nueva delincuencia no puede en y por sí misma detener la comisión de lo hemos llamado **"Delito Informatico"**, pero consideramos que a la larga la nueva legislación reduciria el número de esta clase de ilicitos.

5.5 REFORMAS Y ADICIONES A LAS LEGISLACIONES PENALES MEXICANAS

Después de este estudio así como la investigación y análisis adquirido por diferentes países al enfrentar el *delito informático* y la forma en que está siendo regulada esta problemática en México, además del evidente incremento de esta situación, es necesario a pesar de que en el país el *delito informático* no ha alcanzado el grado de peligrosidad existente en esos países regular penalmente las conductas ilícitas derivadas del uso de la computadora, como se analizo anteriormente.

En primer término, la difusión a las empresas, organismos, dependencias, particulares y a la sociedad en general, contribuirá notoriamente al nivel de concientización sobre el problema que nos ocupa. El siguiente paso dentro de la investigación será dar a conocer las medidas preventivas que se deben adoptar para evitar estas conductas ilícitas.

Sin embargo, con base en que en la Ley Federal del Derecho de Autor se considera como bien jurídico tutelado la propiedad intelectual y que, el bien jurídico tutelado en los *delitos informáticos* es fundamentalmente el patrimonio, se sugiere que en el Título Vigésimo Segundo sobre los *"Delitos en contra de las personas en su patrimonio"* del Código Penal para el Distrito Federal en Materia de Fuero Común y para toda la República en Materia de Fuero Federal se añada un capítulo especial para los *delitos informáticos*.

Teniendo en cuenta también la gravedad que implican los *delitos informáticos*, es necesario que el **Código Penal Federal** incluya figuras delictivas que contengan

los *delitos informáticos* ya que de no hacerlo, la ausencia de figuras concretas que se puedan aplicar en esa materia daría lugar a que los autores de esos hechos quedaran impunes ante la ley, o bien, obligaría a los tribunales a aplicar preceptos que no se ajusten a la naturaleza de los hechos cometidos.

Por otra parte, teniendo presente que el Estado de Sinaloa a través de su Congreso Local ha legislado sobre el tema de *delitos informáticos*, contemplando de forma general una amplia variedad de los mismos y estableciendo las sanciones correspondientes, se establece que es necesario que con objeto de que se evite un conflicto de competencia entre los congresos locales y el de la Unión, éste con base en las facultades que la Constitución Federal le confiere, establezca los criterios necesarios para delimitar, dada la naturaleza de los *delitos informáticos*, que pueden emplear para su ejecución las vías generales de comunicación entre otros elementos, la jurisdicción federal y local de estos ilícitos.

CONCLUSIONES

PRIMERA. Respecto a la seguridad jurídica y validez legal de un documento emitido por un medio electrónico (llámese computadora), es necesario, normar las bases de seguridad y auditoría, bajo las cuales se ha de elaborar un sistema informático cuyo objetivo sea la emisión de documentos, donde se contemplen las características de seguridad y auditoría de los procesos a los que sean sometidos los documentos. Después de tener las normas mencionadas anteriormente, se podrá hablar de confiabilidad jurídica y fincar responsabilidades sobre alteración de documentos electrónicos o negligencia en la preparación, diseño o elaboración del sistema.

SEGUNDA. Que se convoque a los interesados a formar grupos de trabajo en el ámbito académico, de gobierno y empresarial para la creación de propuestas concretas en las que se propongan estándares, análisis, estrategia nacional de contenidos, sobre el problema de la seguridad informática.

TERCERA. Se propone la realización de foros trimestrales en diversos puntos del país enfocados al interés por México y al impacto en el desarrollo y bienestar social, en los cuales se dé una participación abierta sobre el problema que nos rodea.

CUARTA. Se requiere de una determinación de acceso a Internet de contenido nacional en español, en proyectos tendientes a terminar con el analfabetismo informático y a propiciar la promoción de cultura tecnológica.

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

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

SÉPTIMA. Nuevas formas de hacer negocios como el comercio electrónico puede que no encuentre el eco esperado en los individuos y en las empresas hacia los que va dirigido ésta tecnología, por lo que se deben crear instrumentos legales efectivos que ataquen ésta problemática, con el único fin de tener un marco legal que se utilice como soporte para el manejo de éste tipo de transacciones.

OCTAVA. La responsabilidad del auditor informático no abarca el dar solución al impacto de los delitos o en implementar cambios; sino más bien su responsabilidad recae en la verificación de controles, evaluación de riesgos, así como en el establecimiento de recomendaciones que ayuden a las organizaciones a minimizar las amenazas que presentan los delitos informáticos.

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

DECIMA. Se propone para el caso de reglamentación al Sector Privado, que adjunto al dictamen fiscal del auditor externo se certifique que la compañía cuente con las licencias de uso del software; en caso de no existir dictamen fiscal, se debe incluir en la declaración anual, una relación de software con número de licencia de uso. Dicha relación debe ser verificable por la autoridad.

DECIMA PRIMERA. Con respecto al combate a la piratería se sugieren la auditoria informática, en los siguientes aspectos: realizadas por alumnos y maestros, esta es prácticamente imposible ya que las escuelas e institutos son los

primeros en fomentar la piratería, es necesario pues, iniciar las auditorias en estos lugares; y, auditoria por programas (organismo auditor).

DECIMA SEGUNDA. La actual situación del país hace que a la mayoría de las personas no cuente con posibilidades de adquirir una computadora; por lo que es más difícil adquirir software. Se ha pensado en campañas en T.V., radio y periódico para crear conciencia sobre el delito informático así mismo que pueda haber facilidades para adquirir software como lo hay para comprar hardware.

REFLEXIÓN FINAL

La humanidad del derecho no puede quedarse atrás a estos grandes desafíos que nos impone las nuevas generaciones y los avances tecnológicos.

Tenemos que empezar a trabajar generando modelos de conocimientos, respuestas coherentes y métodos de análisis. No importa desde que postura partamos. Pero tenemos que comenzar a estudiar un nuevo mundo, que para algunos es estupendo e importante y para otros se presenta oscuro y deshumanizado.

Sin embargo la ciencia jurídica debe estar en este lugar aquí y ahora afrontando los nuevos retos que impone la vida y moderando los conflictos sociales por que todo esto nos lleva a proteger los intereses individuales y colectivos del hombre.

BIBLIOGRAFÍA

AMOROSO Fernández, Yarina. "La informática como objeto de derecho. Algunas consideraciones acerca de la protección jurídica en Cuba de los Datos Automatizados" en Revista Cubana de Derecho. Unión Nacional de Juristas de Cuba. No. 1. Habana, Cuba. 1991.

ANIYAR DE CASTRO, Lolita. El delito de cuello blanco en América Latina: una investigación necesaria. ILANUD AL DIA. No.8 Agosto 1980. San José, Costa Rica.

ARTEGA S., Alberto. "El delito informático: algunas consideraciones jurídico penales" Revista de la Facultad de Ciencias Jurídicas y Políticas. No. 68 Año 33. Universidad Central de Venezuela. 1987. Caracas, Venezuela.

Articulo del Dr. Carlos M. Jarque, Presidente del INEGI, en el Foro de Consulta sobre "Derecho e Informática, en el Boletín de Política Informática," No. 7, año XIX, 1996.

Articulo publicado por el plan nacional de desarrollo (INEGI), sobre el "derecho y la informática 1995-2000."

BIERCE, B. William. "El delito de violencia tecnológica en la legislación de nueva York" Derecho de la Alta Tecnología. Año 6 No. 66 Febrero 1994. Estados Unidos.

CASTELLANOS Tena, Fernando, Lineamientos Elementales de derecho penal, Editorial Porrúa, México 1978.

Código de Ética y Conducta Profesional de la Academia Mexicana de Informática citado por Alexander Díaz García (Elementos de la Informática Jurídica).

COMISION DE LAS COMUNIDADES EUROPEAS. "Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones." Contenidos ilícitos y nocivos en Internet. Bruselas, 16.10.1996 COM (96) 487 final.

CORREA M. , Carlos Derecho Informatico, Buenos Aires, Ed. Depalma, 1987.
DE LA CUADRA, Enrique. "Regulación jurídica de la informática computacional" Temas de Derecho Año II No. 3, 1987. Universidad Gabriela Mistral. Santiago de Chile.

DE PINA VARA, Rafael, Diccionario de Derecho, Ed. Porrúa, México, 1996.
DEL PONT K., Luis Marco y NADELSTICHER Mitrania, Abraham, "Delitos de cuello blanco y reacción social", Instituto Nacional de Ciencias Penales. México. 1981.

Exposición de motivos de la Comisión de Justicia de la Cámara de Diputados Doc.223/LVI/97 (II. P.O. Año III) DICT. que contiene el proyecto de decreto por el que se reforman la fracción III del articulo 231 de la Ley Federal del Derecho de Autor así como la fracción III del artículo 424 del Código Penal para el

Distrito Federal en Materia del Fuero Común y para toda la República en Materia del Fuero Federal.

Exposición de motivos de la Comisión de Justicia de la Cámara de Diputados Doc. 184/LVI/96 (I. P.O. Año III) DICT. durante el análisis de la Ley Federal de Derecho de Autor.

FERNANDEZ Calvo, Rafael. "El tratamiento del llamado "delito informático" en el proyecto de ley Orgánico del Código Penal: reflexiones y propuestas de la CLI (Comisión de libertades e informática" en Informática y Derecho.

GARCÍA Fabián y Pablo Palazzi, "Consideraciones para una reforma penal en materia de seguridad y virus informáticos", Ponencia presentada en España en 1995.

GARVARINO, Álvaro, Cúrvelo, Carmelo, et all. "Nuevas normas jurídicas en materia informática" Revista de la Asociación de Escribanos del Uruguay. Vol. 76 No. 1 - 6. Enero-Junio 1999. Montevideo, Uruguay.

Hackers. Historias prohibidas. Revista Electrónica en Español WORLD.

HANCE, Olivier. Leyes y Negocios en Internet. México. De. Mc Graw Hill Sociedad Internet. México. 1996.

JIMÉNEZ de Asúa, Luis, La Ley y el Delito, Editorial Hermes, Argentina, 1954,

LIMA DE LA LUZ, María. "Delitos Electrónicos" en Criminalia. México. Academia Mexicana de Ciencias Penales. Ed. Porrúa. . No. 1-6. Año L. Enero-Junio 1984.

LOPEZ VERGARA, Jorge, Introducción al Estudio de la Criminología, Revista Mexicana de Derecho Penal, 5ª. Época, numero 4, México 1978.

MARCHIORI, Hilda, Personalidad del delincuente , 3ra. México , Ed. Porrúa, 1985.

MIR PUIG, S (Comp.) Delincuencia Informática. Promociones y Publicaciones Universitarias. Barcelona, 1992.

NACIONES UNIDAS. Revista Internacional de Política Criminal. Manual de las Naciones Unidas sobre "Prevención del Delito y Control de delitos informáticos." Oficina de las Naciones Unidas en Viena. Centro de Desarrollo Social y Asuntos humanitarios. Nos.43 y 44. Naciones Unidas, Nueva York.1994.

NORA, Sinon y MINC, Alain. La Informática de la sociedad, México, Fondo cultural Economía, 1981.

OSORIO Y NIETO, Cesar Augusto, Síntesis de Derecho Penal , Ed. Trillas, México 1984.

Prevención del delito y justicia penal en el desarrollo informatico nacional: . Documento de trabajo preparado por la Secretaria (A/CONF.144/5). Octavo Congreso sobre Prevención del delito y tratamiento del delincuente. Guadalajara 2001.

Primer Congreso Nacional de Delitos Cibernéticos. México. 2000.

Robo y Manipulación informática, Articulo publicado por el instituto de seguridad de computadoras, Estados Unidos de Norte América año 2000.

ROJAS PEREZ, Palacio Alfonso, Delitos de Cuello blanco, México Ed. Joaquín porrúa 1986.

SARZANA, Carlos. "Criminalitá e tecnología" en Computers Crime. Rassagna Penitenciaria e Criminología. Nos. 1-2. Ano 1. 1979. Roma, Italia.

TELLEZ Valdés, Julio, " Delincuencia automatizada: los virus informáticos y el terrorismo por computadora." Tomado del libro Estudios Jurídicos en memoria de Jorge Barrera Graf. Ed. Porrúa, México, D.F., 1993.

TÉLLEZ, Valdez Julio. Derecho Informatico, 2ª. Ed. México. Ed. Mc Graw Hill 1996.

TONIATTI, Roberto. "Libertad informática y derecho a la protección de los datos personales: principios de legislación comparada". Revista Vasca de Administración Pública. No. 29, Enero-Abril, 1991, España.

VIVANTI, Michel, "Droit de Informatique Paris," Edit. Lamy, S.A , 1986.

OTRAS FUENTES

http://www.monografia.com.

Código de Ética y Conducta Profesional de la Academia Mexicana de Informática. www.amiac.cm.

http://www.netle-ec.com.

http://personales-ciudad.com.ar/reble/thaissdelitos informaticos.htm

http://tiny.uasnet.mx/index.htm

http://rtn.net.mx/ocde/index.html.

http://www.onnet.es/04001002.htm

L E G I S L A C I O N E S

Constitución Política de Los Estados Unidos Mexicanos

Código Penal Federal vigente

Código Penal para el Distrito Federal.

Código Penal y de Procedimientos Penales del Estado de Sinaloa. Editorial. Anaya 1996. México.

Ley Federal del Derecho de Autor. Diario Oficial de la Federación. Martes 24 de diciembre de 1996.

Ley de Vías Generales de Comunicación. Colección Porrúa.

Legislación sobre propiedad industrial. Editorial Porrúa. 19ª edición. México.

Tratado de Libre Comercio (TLC) Parte 3. Diario Oficial de la Federación. Lunes 20 de diciembre de 1993.

Ley contra la criminalidad Economía, 1966.

TRAMITE PARLAMENTARIO No. 19 Ley Nacional de Informática, Argentina, 1986.

Código Civil Argentino

Código Penal Australiano

Ley Contra delitos informaticos Chile, 1993

Código Penal Español

Acta Federal de Abuso Computacional, 1994 , EE.UU

Ley relativa al fraude informático 1998

Ley de Abusos Informáticos de 1991

Ley de Delitos Informáticos de 1993