CARABINEROS DE CHILE

ACADEMIA DE CIENCIAS POLICIALES

DEPTO. DE INGENIERIA

"DELITOS EMERGENTES EN INTERNET Y EL DESAFIO DE CARABINEROS DE CHILE EN LA PREVENCIÓN Y CONTROL EN LA ERA INFORMÁTICA"

SEMINARIO DE TITULO

PRESENTADO EN CONFORMIDAD A LOS REQUISITOS

PARA OBTENER EL

TITULACIÓN DE INGENIERO EN INVESTIGACIÓN POLICIAL

PROF. GUIA: DON ANDRES COO

CAPITAN SR. JOSE ALFONSO TOLEDO DUMENES

AÑO 2001

AGRADECIMIENTOS

A mi Madre y mi Padre.
y quienes han estado a mi lado, alentando
y apoyando en este duro camino
al conocimiento

INDICE TEMATICO

CAPITULO II

ANTECEDENTES HISTORICOS

ANTECEDENTES GENERALES DEL DELITO INFORMATICO

ANTECEDENTES CRIMINOLOGICOS FRENTE A DELITOS INFORMATICOS O CIBERCRIMEN.

ANTECEDENTES LEGALES

ANTECEDENTES DE LA PROBLEMÁTICA INTERNACIONAL

- ACCIONES REALIZADAS POR LA COMUNIDAD INTERNACIONAL PARA LA PREVENCIÓN Y CONTROL FORMAL E INFORMAL DEL CIBERCRIMEN.

- RESPONSABILIDADES ENTREGADAS A LOS ORGANISMOS POLICIALES EXTRANJEROS.

ANTECEDENTES DE LA PROBLEMÁTICA NACIONAL

- INFOESTRUCTURA PARA LA ECONOMÍA DIGITAL

- ECONOMIA DIGITAL

LA SEGURIDAD INFORMÁTICA EN LA ECONOMÍA DIGITAL

BRECHAS DE SEGURIDAD

PROYECCIONES DEL COMERCIO ELECTRÓNICO EN CHILE

TAMAÑO Y PROYECCIONES DE LA ECONOMÍA DIGITAL EN CHILE

CAPITULO III

LA SITUACION INSTITUCIONAL Y POLICIAL EN CHILE

CARABINEROS DE CHILE Y SU INCORPORACIÓN AL PROCESO DE PREVENCIÓN Y CONTROL SOCIAL DEL CIBERCRIMEN

RESPONSABILIDADES ENTREGADAS A LOS ORGANISMOS POLICIALES CHILENOS

CAPITULO IV

CONCLUSIONES

PROPUESTAS AMBITO DE CARABINEROS DE CHILE

PROPUESTAS AMBITO ACADEMICO

CAPITULO I

1.- INTRODUCCIÓN

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 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 Chile, 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 día 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 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 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 del comercio electrónico.

2.- PLANTEAMIENTO DEL PROBLEMA

Nuestra era, se caracteriza por un creciente acceso a la tecnología y a una globalización social de la información y de la economía. El desarrollo tecnológico y el mayor uso de redes abiertas, como Internet, en los próximos años, proporcionarán oportunidades nuevas e importantes y plantearán nuevos desafíos. La infraestructura de la información se ha convertido en una parte vital del eje de nuestras economías. Los usuarios deberían poder confiar en la disponibilidad de los servicios informativos y tener la seguridad de que sus comunicaciones y sus datos están protegidos frente al acceso o la modificación no autorizados. El desarrollo del comercio electrónico y la realización completa de la sociedad de la información dependen de ello.

El uso de las nuevas tecnologías digitales y de la telefonía inalámbrica ya se ha generalizado. Estas

tecnologías nos brindan la libertad para poder movernos y permanecer comunicados y conectados con miles de servicios construidos sobre redes de redes. Nos dan la posibilidad de participar; de enseñar y aprender, de jugar y trabajar juntos, y de intervenir en el proceso político. A medida que las sociedades dependen cada vez más de estas tecnologías, será necesario utilizar medios jurídicos y prácticos eficaces para prevenir los riesgos asociados. 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.

El enfoque clásico de la seguridad exige una compartimentación organizativa, geográfica y estructural estricta de la información, según su sensibilidad y su categoría. Esto no es ya prácticamente posible en la práctica en el mundo digital, puesto que el tratamiento de la información se distribuye, se prestan servicios a usuarios móviles, y la inter operabilidad de los sistemas es una condición básica. Los enfoques tradicionales de la seguridad son sustituidos por soluciones innovadoras basadas en las nuevas tecnologías. Estas soluciones implican el uso del cifrado y las firmas digitales, de nuevos instrumentos de autenticación y de control del acceso, y de filtros de software de todo tipo. Garantizar infraestructuras de información seguras y fiables no sólo exige la aplicación de diversas tecnologías, sino también su correcto despliegue y su uso efectivo. Algunas de estas tecnologías existen ya, pero a menudo los usuarios no son conscientes de su existencia, de la manera de utilizarlas, o de las razones por las que pueden ser necesarias, esta última circunstancia esta muy fuertemente arraigada 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.

3.- RELEVANCIA DEL PROBLEMA

La delincuencia informática se comete en el ciberespacio, y no se detiene en las fronteras nacionales convencionales. En principio, puede perpetrarse desde cualquier lugar y contra cualquier usuario de ordenador 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 con vocación internacional frente a los nuevos retos de la seguridad de la red y la delincuencia informática. En los países, las reacciones frente a la delincuencia informática se centran en el derecho nacional, descuidando medidas alternativas de prevención. A pesar de los esfuerzos de las organizaciones internacionales y supranacionales, las diversas leyes nacionales de todo el mundo ponen de manifiesto considerables diferencias, especialmente en 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 las investigaciones en redes internacionales), la jurisdicción en materia penal, y con respecto a la responsabilidad de los proveedores de servicios intermediarios por una parte y los proveedores de

contenidos por otra.

A escala internacional y supranacional, se ha reconocido ampliamente la necesidad de luchar eficazmente contra la delincuencia informática, y diversas organizaciones han coordinado o han intentado armonizar actividades al respecto.

Todas estas acciones internacionales no han logrado calar en nuestra realidad y lograr cambiar la nula percepción de inseguridad que sentimos frente a estos nuevos hechos, cabe destacar la reciente creación de parte de la Policía de Investigaciones de la Brigada del Cibercrimen, que tiene como fundamento la de perseguir y llevar ante los Tribunales de Justicia a los hechores de este tipo de acciones, que anualmente pueden causar daños económicos superiores a los US$ M30.

4.- HIPOTESIS

No se presentan por las características de la investigación exploratoria.

5.- METOLOGIA DE LA INVESTIGACIÓN:

Descripción :

Para el desarrollo del presente trabajo de Tesis, se opto por la siguiente metodología:

- Se realizo una investigación bibliográfica, de recopilación de material escrito sobre la percepción de seguridad que tienen los usuarios de Internet, y de entrevista desde el punto de vista económico, social, policial y judicial.

- Con los datos obtenidos, se realizó una selección de material escrito, emanado de diversas fuentes externas a nuestro país, provenientes de países con mayor desarrollo y experiencias en esta área del crimen tecnológico o cibercrimen.

- Se participa activamente en una empresa que entrega servicios de seguridad informática, a fin de realizar una investigación exploratoria de la seguridad, metodología en uso por los llamados “hackers”.

6.- OBJETIVO:

6.1.-OBJETIVOS GENERALES

- Dar un acercamiento sobre la realidad que acontece en Chile sobre la problemática que afecta a nuestra sociedad y que dice relación con 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 informática en Carabineros de Chile.

- Dar una propuesta real de acción para Carabineros de Chile con el fin que sus recursos humanos y materiales se aboquen al estudio, análisis y evaluación de esta problemática delictual, desarrollando los cursos necesarios para no ser sorprendidos y sobrepasados por esta nueva realidad nacional e internacional.

6.2.- OBJETIVOS ESPECIFICOS:

- Realizar una síntesis de las fortalezas y debilidades que presenta Carabineros de Chile para enfrentar la problemática de los delitos informáticos.

- Realizar en el plano externo de la sociedad chilena, las oportunidades y amenazas a que se ve enfrentada Carabineros de Chile, para enfrentar la problemática de los delitos informáticos.

- Determinar sobre la base de legislación comparada, la trascendencia que ha adoptado el tema de los delitos informáticos en otras áreas geográficas del mundo.

- La propuesta conveniente para que Carabineros de Chile, asuma su responsabilidad como ente Cooperador de la Justicia y elemento fundamental en el control social formal y acepte el desafío de ingresar a un nuevo campo de estudio y acción de esta nueva topología de delincuencia emergente.

- Carabineros de Chile, debe enfrentar la globalización de la informática, económica y social, con sus medios debe ponerse a la vanguardia en Chile como el resto de América Latina en el estudio, análisis y control de estos hechos que transgreden la realidad social.

- Realización de una metodología científico / técnico, en el ámbito de la informática, a fin de adaptar nuestra labor policial preventiva / investigativa, acorde a esta nueva y muy singular área de trabajo.

CAPITULO II

DESARROLLO DEL TEMA

1.- ANTECEDENTES HISTORICOS

La Agencia de Proyectos de Investigación Avanzada (**ARPA**) se inició en el Departamento de Defensa de los Estados Unidos en los últimos años de la década de los cincuenta para investigar los campos de ciencia y tecnología militar. El objetivo de la propuesta era plantear una red que tuviera la máxima resistencia ante cualquier ataque enemigo. Se suponía que una red de comunicaciones, por si misma, no es fiable debido a que parte de ella podría ser destruida durante un ataque bélico.

Por lo tanto, cada nodo debería 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 Físico 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 envío de paquetes de información, realizado por Lawrence. Roberts, fue presentado en la ARPA. La red se llamó ARPANET.

Al año siguiente, el Departamento de Defensa dio el visto bueno para comenzar la investigación en ARPANET. El primer nodo, fue 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 Utah. Estos sitios (como denominamos a los nodos) constituyeron la red original de cuatro nodos de **ARPANET**. Los cuatro sitios podían transferir datos en ellos en líneas de alta velocidad para compartir recursos informáticos.

El comienzo de la década de los setenta vio el crecimiento de la popularidad del correo electrónico sobre

redes de almacenamiento y envío. En 1971, **ARPANET** había crecido hasta 15 nodos con 23 ordenadores hosts (centrales). En este momento, los hosts comienzan a utilizar un protocolo de control de redes, pero todavía falta una estandarización. Además, había muy diferentes tipos de hosts, por lo que el progreso en desarrollar los diferentes tipos de interfaces era muy lento.

En 1972 Larry Roberts de DARPA decidió que el proyecto necesitaba un empujón. Organizó la presentación de **ARPANET** en la Conferencia Internacional sobre Comunicaciones por Ordenador. A partir de esta conferencia, se formó un grupo de trabajo internacional para investigar sobre los protocolos de comunicación que permitirían 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 v Newman (BBN) produjeron una aplicación de correo electrónico que funcionaba en redes distribuidas como **ARPANET**. El programa fue un gran éxito que permitió a los investigadores coordinarse v 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 expansión era muy fácil debido a su estructura descentralizada.

En 1974 se estableció el Transmission Control Protocol (TCP), creado por Vinton Cerf y Bob Kahn que luego fue desarrollado hasta convenirse en el Transmission Control Protocol/Internet Protocol (TCP/IP). TCP convierte 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 envíos de datos, asegurando que los paquetes de información separados se encaminan por vías separadas a través de diversos nódulos, e incluso a través de múltiples redes con arquitecturas distintas.

En julio de 1975 ARPANET fue transferido por DARPA a la Agencia de Comunicaciones de Defensa.

El crecimiento de ARPANET hizo necesario algunos órganos de gestión: el Internet Configuration Control Board fue 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 Society.

ARPANET en sí mismo permaneció estrechamente controlado por el DoD hasta 1983 cuando su parte estrictamente militar se segmentó convirtiéndose en MILNET. La "European Unix Network" (EuNet), conectado a ARPANET, se creó en 1982 para proporcionar servicios de correo electrónico y servicios Usenet a diversas organizaciones usuarias en los Países Bajos, Dinamarca, Suecia e Inglaterra.

En 1984 el número de servidores conectados a la red había ya superado los 1.000. Dado que el software

de TCP/IP era de dominio público y la tecnología básica de Internet (como ya se denominaba esta red internacional extendida) era algo anárquica debido a su naturaleza, era difícil evitar que cualquier persona en disposición del necesario hardware (normalmente en universidades o grandes empresas tecnológicas) se conectase a la red desde múltiples sitios.

En 1986, la National Science Foundation (NSF) de EE.UU. inició el desarrollo de NSFNET que se diseñó originalmente para conectar cinco superordenadores. Su interconexión con Internet requería unas líneas de muy alta velocidad. Esto aceleró el desarrollo tecnológico de INTERNET y brindó a los usuarios mejores infraestructuras de telecomunicaciones. Otras agencias de la Administración norteamericana entraron en Internet, con sus inmensos recursos informáticas y de comunicaciones: NASA y el Departamento de Energía.

El día 1 de noviembre de 1988 Internet fue "infectada" con un virus de tipo "gusano". Hasta el 10% de todos los servidores conectados fueron afectados. El acontecimiento subrayó la falta de adecuados mecanismos de seguridad en Internet, por lo cual DARPA formó el Computer Emergency Reponse Team (CERT), un equipo de reacción rápida que mantiene datos sobre todas las incidencias en red y sobre las principales amenazas.

En 1989 el número de servidores conectados a Internet alcanza ya los 100.000. En este mismo año, se inauguró también la primera conexión de un sistema de correo electrónico comercial a Internet (MCI y Compuserve). Una nueva época estaba a punto de empezar, la de la explotación

ARPANET como entidad se extinguió en 1989/90, habiendo sobrepasado 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 mejoraron notablemente a través de nuevos órganos más representativos de la utilización actual de la red.

En 1990 redes de diversos países como España, Argentina, Austria, Brasil, Chile, Irlanda, Suiza y Corea del Sur se conectaron también a NSFNET.

En 1991 se retiraron las restricciones de NFS al uso comercial de INTERNET. Ese mismo año también se Conectaron más países a la NSFNET incluyendo: Croacia, Hong Kong, República Checa, Sudáfrica, Singapur, Hungría, Polonia, Portugal, Taiwan y Túnez.

En 1992 el número de servidores conectados a INTERNET sobrepasaba la cifra de un millón de servidores. En ese año, la Sociedad de INTERNET (ISOC) se formó para promocionar el intercambio global de información. La Internet Architecture Board (IAB), fue reorganizada para llegar a formar parte del ISOC.

Como acontecimiento clave en la historia reciente de Internet, también en 1992 se desarrolló la World Wide Web en el Laboratorio Europeo de Física 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 sobrepasa los 2.000.000. También NSF patrocina la formación de una nueva organización, ínterNIC, creada para proporcionar servicios de registro en Internet y bases de datos de direcciones. El conocido navegador WWW 'Mosaic" se desarrolló en el National Center for Supercomputing.

El número de servidores de Internet alcanza los **3.800.000** en 1994. Las primeras tiendas Internet empiezan a aparecer junto con "emisores" de radio on-line.

En 1995 había más de 5 millones de servidores conectados a Internet. La espina dorsal de NSFNET empezaba a ser sustituido por proveedores comerciales interconectados.

2.- 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 o hurto, fraudes, falsificaciones, perjuicios, estafa, sabotaje, etcétera. Sin embargo, debe destacarse que el uso de las técnicas informáticas ha creado nuevas posibilidades del uso indebido de las computadoras lo que ha propiciado a su vez la necesidad de regulación por parte del derecho.

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

Por lo que se refiere a las definiciones que se han intentado dar, cabe destacar que **Julio Téllez Valdez** 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".

Ø Para **Carlos Sarzana**, en su obra Criminalità e tecnología, los crímenes por computadora comprenden "cualquier comportamiento criminógeno en el cual la computadora ha estado involucrada como material o como objeto de la acción criminógena, o como mero símbolo".

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

Ø **Rafael Fernández Calvo** define al delito informático como "la realización de una acción que, reuniendo las características que delimitan el concepto de delito, se ha llevado a cabo utilizando un elemento informático o telemático contra los derechos y libertades de los ciudadanos definidos en el título 1 de la **Constitución Española.**

Ø **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".

Ø **Julio Téllez Valdez** 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".

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 consecuencia el presente trabajo se entenderá como "delitos informáticos" **todas aquellas conductas ilícitas susceptibles de ser sancionadas por el derecho penal, que hacen uso indebido de cualquier medio informático.**

3.- ANTECEDENTES CRIMINOLOGICOS FRENTE A DELITOS INFORMATICOS.

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.

En la mayoría de las naciones occidentales existen normas similares a los países europeos. Todos estos enfoques están inspirados por la misma de 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 TELLEZ VALDEZ 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)". 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".

Según TELLEZ VALDEZ, este tipo de acciones presenta 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) puede llegar a cometerlas.

b. Son acciones ocupacionales, en cuanto a que muchas veces se realizan cuando el sujeto se haya 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 económicos " al hechor.

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.

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, el autor escogido clasifica a estos delitos, de acuerdo con dos criterios:

1. 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 ficticia

h. Uso no autorizado de programas de computo.

i. Introducción de instrucciones que provocan "interrupciones" en la lógica interna de los programas.

j. Alteración en el funcionamiento de los sistemas, a través de los virus informáticos.

k. Obtención de información residual impresa en papel luego de la ejecución de trabajos.

l. Acceso a áreas informatizadas en forma no autorizada.

m. Intervención en las líneas de comunicación de datos o teleproceso.

2.- 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.

a. Daño a la memoria.

b. Atentado físico contra la máquina o sus accesorios.

c. Sabotaje político o terrorismo en que se destruya o surja un apoderamiento de los centros neurálgicos computarizados.

d. 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:

Ø Acceso no autorizado: Uso ilegitimo de passwords y la entrada de un sistema informático sin la autorización del propietario.

Ø Destrucción de datos: Los daños causados en la red mediante la introducción de virus, bombas lógicas, etc.

Ø Infracción al copyright de bases de datos: Uso no autorizado de información almacenada en una base de datos.

Ø Interceptación de e-mail: Lectura de un mensaje electrónico ajeno.

Ø Estafas electrónicas: A través de compras realizadas haciendo uso de la red.

Ø 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:

Ø Espionaje: Acceso no autorizado a sistemas informáticos gubernamentales y de grandes empresas e interceptación de correos electrónicos.

Ø Terrorismo: Mensajes anónimos aprovechados por grupos terroristas para remitirse consignas y planes de actuación en el ámbito internacional.

Ø Narcotráfico: Transmisión de fórmulas para la fabricación de estupefacientes, para el blanqueo de dinero y para la coordinación de entregas y recogidas.

Ø 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.

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 los diferencia entre sí, es la naturaleza de los delitos cometidos. De esta forma, la persona que "ingresa" 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.

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 fueron 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.

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", los estudiosos en la materia los han catalogado como "delitos de cuello blanco" término introducido por primera vez por el criminólogo norteamericano Edwin Sutherland en el año de 1943.

Efectivamente, este 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, 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. Sin embargo, la cifra 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 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.

Este nivel de criminalidad 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 el agresor y la víctima estén sujetos a leyes nacionales diferentes. 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.

4.- ANTECEDENTES LEGALES

4.1.- PROBLEMAS JURÍDICOS DE LA INTERNET

Los problemas jurídicos que se plantean a raíz de las actividades en el ciberespacio son de variada naturaleza. Muchos de ellos provienen del uso de nombres identificatorios de los servidores, que chocan con derechos de propiedad industrial previamente adquiridos, como las marcas comerciales registradas. Otros problemas provienen de la información que puede ser "publicada" en la red, 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

prohibidas (como las apuestas), altamente reguladas (como las actividades bancarias y del mercado de capitales) o fuertemente protegidas (como la diseminación de datos privados), la existencia de legislaciones ordinarias independientes de los países, la comisión de delitos que no reconocen la existencia de las fronteras tradicionales entre países. Por último, 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 jurisdicción aplicable a dicha actividad, las consecuencias fiscales, etc.

4.2.- LOS NOMBRES DE DOMINIO Y LAS MARCAS COMERCIALES

Uno de los problemas jurídicos más debatidos en los últimos años en materia de actividad en el ciberespacio es el derivado del sistema de identificación de los participantes en la red. En efecto, cada recurso en la Internet, tal como una página Web o un archivo con información, tiene su propia dirección, técnicamente conocida como "ubicador de recursos uniforme" (URL), para ser identificada.

Uno de los componentes de esta dirección es el llamado "nombre de dominio". Cada servidor en la red tiene asignada una serie de números o dirección Protocolo de Internet (IP), tal como "**200.10.184.6**". Estos números se vinculan a una dirección Domain Name Server (DNS) que es fácilmente leíble y recordable (el nombre de dominio). A modo de ilustración, la serie de números antes mencionada corresponde a la dirección de La Corporación Administrativa del Poder Judicial de Chile, (www.cortesuprema.cl), que es el nombre de dominio del IP señalado. Dado que sería muy difícil recordar cada vez la serie de números que forma parte de cada dirección IP, el sistema de nombres de dominio permite elegir un nombre reconocible, distinguible, en el ciberespacio.

La función que cumplen los nombres de dominio, esto es, distinguir a una página Web de otra, constituye, a su vez, la función fundamental de las marcas comerciales. Un primer problema de los nombres de dominio es que dos empresas distintas pueden tener un signo distintivo idéntico: un nombre de dominio y una marca comercial. Un segundo problema está dado por el hecho de que la protección marcaría está limitada al territorio en que se encuentra inscrita, mientras que el nombre de dominio registrado rige para todo el ciberespacio. Otro problema está dado porque la normativa para el registro de las marcas comerciales es diferente del aplicable a los nombres de dominio, que es mucho más flexible y simple. Por ejemplo, las marcas pueden inscribirse en cuarenta y dos clases, mientras que los nombres de dominio sólo en uno, lo que no permite que coexistan nombres de dominio iguales, aunque se trate de empresas que tengan giros completamente distintos; los nombres de dominio se inscriben sobre la base del "primero que llega" y los entes encargados del registro no realizan ninguna investigación acerca del

derecho al nombre a ser registrado.

Por otra parte, en el mundo físico es esencial para una empresa contar con una ubicación que le dé prestigio y presencia, lo que suele tener un costo muy alto. Sin embargo, en el mundo virtual, las empresas tienen presencia en el ciberespacio; estas entidades son conocidas por sus nombres de dominio y el diseño de sus páginas Web y no por su ubicación física. Entonces, habiendo millones de páginas Web compitiendo en el ciberespacio, se torna cada vez más importante para una empresa de Internet tener el nombre de dominio apropiado. Esto ha sido reconocido por una multiplicidad de empresas, que han gastado fortunas en dar a conocer sus nombres de dominio y copar el ciberespacio.

Por ello, el registro de un nombre de dominio puede ser un tema muy sensible, sobre todo cuando se trata de uno idéntico al de una marca comercial previamente registrada por un tercero. Esto ha llevado a la formación de la Corporación para los Nombres y Números Asignados en Internet (ICANN), que es responsable de mantener la infraestructura para las direcciones en la Internet. Bajo la ICANN, existe un registro por país administrado por centros de información de red denominados "NIC". Cada registro, que en el caso de Chile es administrado por el Departamento de Ciencias de la Computación de la Universidad de Chile y se denomina "NIC Chile", coordina las direcciones IP con los nombres de dominio registrados en su territorio geográfico (prefijo "cl" para Chile). A su vez, todos los registros acreditados en la ICANN siguen las Reglas Uniformes para la Solución de Controversias sobre Nombres de Dominio (URDP) de 1999, que establece que los conflictos en el registro de nombres de dominio deben ser resueltos por acuerdo mutuo o por sentencia judicial o arbitral, antes que el registro correspondiente pueda cancelar, suspender o transferir un nombre de dominio (www.nic.cl.)

4.3.- EL DERECHO DE AUTOR

Los medios tecnológicos disponibles en la actualidad y que se emplean en el ciberespacio permiten el intercambio de información y productos en forma incorporal. Para hacer posible este tránsito de información, ha sido preciso traducirla a un código binario que permite transmitir imágenes, sonido y texto. Es lo que se denomina "bienes digitales". En general, las legislaciones protegen, bajo la denominación del derecho de autor, todas las creaciones artísticas y científicas, en cuanto a la posibilidad de ser reproducidas por cualquier medio.

En el mundo físico, la protección de las creaciones individuales puede ser perseguida de una forma más o menos sencilla, por cuando éstas constan en una base de corporeidad reconocible, lo que dificulta su reproducción y almacenaje. Sin embargo, en el mundo virtual aquéllas son representadas por una realidad digital, que puede viajar en forma instantánea de un lugar a otro del ciberespacio y pueden ser infinitamente reproducidas sin perder su calidad. Esto es, las creaciones pueden ser desmaterializadas,

haciéndose fácilmente vulnerable el derecho autoral.

Se puede afirmar que la protección del derecho de autor no se ve lesionada *per se* por la actividad en el ciberespacio, sino que es más difícil controlar las infracciones en su contra.

Estos se discuten extensamente en distintos foros internacionales, tales como las Naciones Unidas, la Organización Mundial de Propiedad Intelectual (OMPI), la Organización Mundial del Comercio (OMC) y la Comunidad Económica Europea, generándose diversas propuestas y recomendaciones legislativas.

4.4.- REALIZACION DE ACTIVIDADES ALTAMENTE REGULADAS

Existen muchas actividades lícitas que en Chile requieren de una licencia otorgada por el Estado para poder ser legalmente desempeñadas. Entre estas actividades se encuentran la actividad bancaria (10 DFL Nº 3 del Ministerio de Hacienda de fecha 19 de diciembre de 1997), la aseguradora (DFL Nº 251 del Ministerio de Hacienda de fecha 22 de mayo de 1931), y la intermediadora de valores (Ley Nº 18.045 sobre Mercado de Valores de fecha 22 de octubre de 1981).

En materia de intermediación de valores, las herramientas disponibles hoy en día en la Internet pueden llevar a la conclusión de que las bolsas de valores ya no serán necesarias, porque los inversionistas pueden "encontrarse" sin necesidad de que exista un mercado secundario especial, al menos físicamente. De este modo, se podría establecer un lugar virtual de encuentro entre oferentes y demandantes, donde quienes quieran comprar y vender inscriba sus acciones y un sistema computacional automatizado asigne en forma eficiente las diferentes órdenes de compra y de venta, uniendo las puntas.

Esto haría desaparecer a las bolsas de valores, porque ya no se justifican. Un sistema bien diseñado para la red podría reemplazar todas sus funciones. Si desaparecen las bolsas de valores, los corredores de bolsa también van perdiendo su razón de existir, porque eso significa que los oferentes y demandantes están interactuando en forma directa. En este escenario, su contribución mayor la constituirían las actividades complementarias a su giro, tales como la asesoría financiera, la custodia de valores, etc. Pero aun en ese escenario, en la medida que dichas funciones puedan reemplazarse por servicios en línea, tales como los análisis financieros, empresariales y accionarios, por una parte, y la desmaterialización de los títulos, por otra, la actividad de los intermediarios de valores tenderá a desaparecer. (ver www.cb.cl, www.larrainvial.cl y www.patagon.cl.)

Pero esta actividad, que por los medios tecnológicos empleados pareciera indicar un vuelco hacia la desintermediación, no es otra cosa –hasta el momento– que una manifestación evolutiva del negocio, donde los servicios que antes se prestaban personal o telefónicamente ahora se prestan a través de otro canal, tecnológico y de apariencia acorde con los parámetros de la nueva economía. El punto de quiebre se dará cuando se cree una página que en vez de reunir adolescentes para "chatear" reúna inversionistas para "tradear".

Un primer problema legal que trae esta nueva línea de negocios radica en el hecho que, para poder desarrollar la actividad, la empresa de Internet debe ser autorizada para operar como tal por la Superintendencia de Valores y Seguros (en adelante, la "SVS"), en cumplimiento de las normas del Título VI de la Ley de Mercado de Valores, que impone un monopolio legal a favor de los corredores de bolsa para efectuar la intermediación de acciones (Artículo 24 de la Ley Nº 18.045.), intermediación que sólo puede efectuarse dentro de una bolsa de valores. (Artículo 23 de la Ley Nº 18.045).

Por otra parte, en relación con las actividades de los corredores también existen ciertos problemas legales, ya que el empleo de la red de la Internet para efectuar ofertas de compra y venta de valores supone traspasar las fronteras físicas de los países en que se efectúan dichas ofertas y surge una variedad de preguntas, muchas de las cuales no tienen hoy respuesta normativa.

4.5.- COMERCIO ELECTRONICO

En materia de comercio a través de la Internet, existen variados problemas que pueden surgir. Los más urgentes dicen relación con la formación del consentimiento, la seguridad acerca de la identidad de los contratantes y la prueba de las obligaciones. Otras materias no menos importantes surgen como consecuencia del comercio, esto es, la legislación aplicable al acto o contrato específico, los tribunales competentes y la seguridad de los medios de pago. Así también, las consecuencias fiscales del comercio electrónico, como la aplicación de derechos aduaneros cuando se traduce en la importación de bienes y de impuestos, en los casos que corresponda.

En cuanto a la formación del consentimiento, se requiere de un sistema que, a lo menos, dé seguridad en cuanto a la identidad de la persona que envió el mensaje, a la integridad del mismo, incluyendo que éste no haya sido alterado, a la denominada "no-repudiación", es decir, que el emisor del mensaje no pueda desconocer haberlo enviado y que el destinatario del mismo no pueda desconocer haberlo recibido y, por último, a la confidencialidad del mensaje, es decir, que sólo pueda ser reconocido por el emisor y el destinatario. Las distintas legislaciones han comprendido que el instrumento tecnológico más confiable en esta materia lo constituye la firma electrónica y, particularmente, la firma digital, que contiene un sistema criptográfico que, por medio de claves públicas y privadas, permite a las partes cifrar un determinado mensaje con una clave y descifrarlo con otra. Para poder operar en forma segura, este

sistema requiere de una autoridad certificadora que sea confiable.

En el ámbito internacional, cabe destacar en esta materia la Ley Modelo sobre Comercio Electrónico de la de la Comisión de las Naciones Unidas para el Derecho del Comercio Internacional (UNCITRAL), que regula las firmas y documentos electrónicos y que otorga a los mensajes digitales el mismo valor que a los documentos impresos en papel. La UNCITRAL ha recomendado a los países incorporar las normas de dicha Ley Modelo, con el objeto de facilitar y dar seguridad a las relaciones jurídicas electrónicas. Varios países han adoptado o están estudiando leyes en conformidad a dicha recomendación.

En Chile, este sistema de claves públicas y privadas se encuentra establecido en el Decreto Supremo Nº 81, de 1999, del Ministerio Secretaría General de la Presidencia, que regula el uso de la firma digital y los documentos electrónicos en la administración del Estado, como soporte alternativo a la instrumentalización en papel de las actuaciones de los órganos de la Administración del Estado. Esta norma otorga a la firma digital los mismos efectos que la firma manuscrita, eliminando la necesidad de sellos, timbres y vistos buenos.

Además, siguiendo las recomendaciones de UNCITRAL, recientemente se ha ingresado a tramitación en el Congreso Nacional un proyecto de ley sobre comunicaciones electrónicas (Mensaje N° 158-342, de fecha 09 de Agosto de 2000) , que trata acerca de las transmisiones electrónicas y la prestación de servicios de certificación, incluyendo regulación sobre la formación del consentimiento, el valor probatorio del mensaje de datos, la legislación aplicable y jurisdicción, la propiedad intelectual, los contenidos de los mensajes, la privacidad de los datos y las sanciones aplicables en caso de infracciones a las normas reguladoras de la firma electrónica y los servicios de certificación.

4.6.- PRIVACIDAD PERSONAL.

En la mayoría de los países de la Unión Europea y de América del Norte, se considera a la privacidad como un valor que merece protegerse. Aunque los medios legales de protección varían de un país a otro, en algunos, la privacía esta protegida por ley; en otros, por la jurisprudencia. Estas formas generales de protección implican penalización en el caso de la difusión de mensajes que pueden divulgar información (texto, imágenes, etc.) que constituya una invasión a la privacía. Además, esta queda protegida contra monitoreo electrónico por autoridades gubernamentales y por individuos privados. Por último, esta estrictamente regulado el procesamiento de datos personales, lo cual representa una genuina amenaza a la privacía (tanto en el sector privado como el público, bajo la legislación europea y en el sector público bajo la estadounidense y canadiense), o está sujeto a autorregulación.

Las comunicaciones privada que circulen en Internet están protegidas del monitoreo electrónico por autoridades gubernamentales. El European convention on Human Rights, establece límites muy estrictos a los casos en que tal monitoreo puede ser organizado por los sistemas legales nacionales a los que se sujeta. Sin embargo, la legislación estadounidense parece autorizar a las autoridades de procuración de justicia que revisen, sin orden previa, la identidad de computadoras que establezcan con una computadora bajo vigilancia, pero no el contenido de la comunicación.

También existen excepciones legales a la prohibición del monitoreo electrónico que permiten a los empleadores vigilar cómo usan Internet sus empleados. El alcance de estas excepciones que por lo general se basan en al autorización explícita o implícita del empleado, varía considerablemente de un sistema legal a otro.

4.7.- DERECHO PENAL INFORMATICO y la prueba en el procedimiento penal (procesal penal, según corresponda)

Chile fue el primer país latinoamericano en sancionar una Ley que tipifica figuras penales relativas a la informática, mediante la promulgación de la Ley N°. 19.223, de fecha 28-05-1993, texto que entró en vigencia el 7 de junio de 1993.

En esta ley, la destrucción, inutilización, sustracción, modificación en los sistemas de información, de los de los datos contenidos dentro de una computadora es castigada con penas desde un año y medio a cinco años de prisión. Texto legal de la mayor amplitud, pero acorde a los conocimientos actuales imperfecta, toda vez que el simple daño material a un computador, se podría considerar como tipificado dentro del ámbito de esta ley, pero no considera situaciones como la transmisión e intercepción en las redes de comunicaciones (Internet), ni aspectos del comercio electrónico. Dentro de esas consideraciones se encuentran todos los virus, programas ejecutables, virus troyanos (gusanos).

Esta ley, en el Art. 1º, 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. 3º tipifica la conducta. maliciosa que altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información.

En el ámbito del Código de Procedimiento Penal y Código de Procesal Penal (vigente en las regiones IV

y IV), a fin de poder lograr la observación y admisión de elementos electrónicos o pruebas digitales para la comprobación de los hechos punibles que hace alusión la Ley de Delitos Informáticos, de admitir analógicamente documentos no contemplados dentro de los medios de prueba, ha sido avalada por los Tribunales. Por ello, en los casos en que se presentaban esos documentos, por ejemplo, una fotografía, se les regulaba como instrumentos, y así, en el proceso civil se les aplicaban las disposiciones de los artículos 342 a 355 del Código de Procedimiento Civil, y en el proceso penal, los artículos 184 a 188 del Código de Procedimiento Penal. Todo esto producía dificultades especialmente cuando se objetaban los documentos. Imperaban, entonces, las pruebas periciales y de presunciones.

Sin embargo, con la Ley N° 18.857, que reformó el Código de Procedimiento Penal en 1989, se mejoró esta situación en el proceso penal, especialmente en lo que se refiere a los documentos, admitiendo como elementos de prueba *"las películas cinematográficas, fotografías, fonografías, y otros sistemas de reproducción de la imagen y del sonido, versiones taquigráficas y, en general, cualquier medio apto para producir fe"* (artículo 113 bis).

A su vez, la reforma al artículo 113 permite al juez, para el esclarecimiento de los hechos, disponer de *"la fotografía, filmación o grabación y, en general, la reproducción de imágenes, voces o sonidos por los medios técnicos que estime convenientes. Asimismo, podrá valerse de resultados obtenidos por la utilización de aparatos destinados a desarrollar exámenes o demostraciones científicas o por medio de la computación"*. Es decir, la ley procesal penal, en su artículo 113 bis, no asimila estos nuevos elementos de prueba a los instrumentos, sino que los considera como documentos y los estima como base de presunciones o indicios, según exista o no una relación precisa y directa entre el hecho acreditado y el que se trata de probar.

Misma consideración y redacción esta presente en el Código de Procesal Penal (vigente en las Regiones IV y IX), en el capítulo IX, De la Prueba, Párrafo 1º, Art. 202º y ss.

En caso que haya objeciones o impugnaciones a las reproducciones acompañadas al proceso, entra en juego la prueba pericial o de técnicos, algunas de las cuales se han reglamentado especialmente por su importancia, como las de los marcadores genéticos sanguíneos en la investigación biológica de la paternidad o la fotografía dactiloscópica como medio de autenticación documental infalible.

En síntesis, la jurisprudencia ha aceptado desde antes de la reforma de la Ley N° 18.857 el concepto amplio de prueba documental para comprender las modalidades de prueba que se mencionan en los artículos 113 y 113 bis del Código de Procedimiento Penal. Con las modificaciones de la ley mencionada no hay problemas en el proceso penal para admitir como elementos de prueba a los documentos electrónicos.

4.8.- LEGISLACION EN OTROS PAISES

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:

Alemania

En Alemania, para hacer frente a la delincuencia relacionada con la informática y con sus 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:

Ø Espionaje de datos (202 a)

Ø Estafa informática (263 a)

Ø 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)

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

Ø 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.

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

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, causación 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 fue 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.

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.

Fue 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 de determinados tipos.

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, 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 sistemas informáticos. El tipo de daños protege cosas corporales contra menoscabos de su sustancia o función de alteraciones de su forma de aparición.

Austria

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

Esta ley contempla los siguientes delitos:

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

Ø 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 o por actuar sobre el curso del procesamiento de datos. Además contempla sanciones para quienes cometen este hecho utilizando su profesión.

Francia

Ley número 88-19 de 5 de enero de 1988 sobre el fraude informático.

Ø Acceso fraudulento a un sistema de elaboración de datos(462-2).- En este artículo se sanciona tanto el acceso al sistema como al que se mantenga en él y aumenta la sanción 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.

Ø Sabotaje informático (462-3).- En este artículo se sanciona a quien impida o falsee el funcionamiento de un sistema de tratamiento automático de datos.

Ø Destrucción de datos (462-4).- En este artículo se sanciona a quien intencionadamente y con menosprecio de los derechos de los demás introduzca datos en un sistema de tratamiento automático de datos o suprima o modifique los datos que este contiene o los modos de tratamiento o de transmisión.

Ø Falsificación de documentos informatizados (462-5).- En este artículo se sanciona a quien de cualquier modo falsifique documentos informatizados con intención de causar un perjuicio a otro.

Uso de documentos informatizados falsos (462-6) En este artículo se sanciona a quien conscientemente haga uso de documentos falsos haciendo referencia al artículo 462-5.

Estados Unidos de Norteamérica

La adopción en los Estados Unidos 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 Toya, etcétera 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, al sistema informático, 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. El acta define dos niveles para el tratamiento de quienes crean virus estableciendo para aquellos que intencionalmente causan un daño por la transmisión de un virus, el castigo de hasta 10 años en prisión federal más una multa y para aquellos que lo transmiten sólo de manera imprudencial la sanción fluctúa entre una multa y un año en prisión.

El Acta de 1994 aclara que el creador de un virus no puede aducir el hecho que no conocía que con su actuar iba a causar daño a alguien o que él solo quería enviar un mensaje.

En opinión de los legisladores estadounidenses, 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.

En el Estado de California, en 1992 se adoptó la Ley de Privacidad en la que se contemplan los delitos informáticos pero en menor grado que los delitos relacionados con la intimidad que constituyen el objetivo principal de esta Ley.

Es importante destacar las enmiendas realizadas a la Sección 502 del Código Penal relativas a los delitos informáticos en la que, entre otros, se amplían los sujetos susceptibles de verse afectados por estos delitos, la creación de sanciones pecuniarias de $10, 000 por cada persona afectada y hasta $50,000 el acceso imprudencial a una base de datos.

El objetivo de los legisladores al realizar estas enmiendas, era el de aumentar la protección a los individuos, negocios y agencias gubernamentales de la interferencia, daño y acceso no autorizado a las bases de datos y sistemas computarizados creados legalmente. Asimismo, los legisladores consideraron que la proliferación de la tecnología de computadoras ha traído consigo la proliferación de delitos informáticos y otras formas no autorizadas de acceso a las computadoras, a los sistemas y las bases de datos y que la protección legal de todos sus tipos y formas, es vital para la protección de la intimidad de los individuos así como para el bienestar de las instituciones financieras, de negocios, agencias gubernamentales y otras relacionadas con el estado de California que legalmente utilizan esas computadoras, sistemas y bases de datos.

Es importante mencionar que en uno de los apartados de esta ley, se contempla la regulación de los virus (computer contaminant), conceptualizándolos aunque no los limita a un grupo de instrucciones informáticas comúnmente llamados virus o gusanos sino que contempla a otras instrucciones designadas a contaminar otros grupos de programas o bases de datos, modificar, destruir, copiar o transmitir datos o alterar la operación normal de las computadoras, los sistemas o las redes informáticas.

España

Ley Orgánica N°. 10 de 1995, de fecha 23 de Noviembre de 1995.

Dentro de la legislación española, podemos distinguir la aplicación de las siguientes medidas en el

ámbito penal.

Ø **Ataques que se producen contra el derecho a la intimidad.** Artículos del 197 al 201 del Código Penal)

Ø **Infracciones a la Propiedad Intelectual a través de la protección de los derechos de autor.** Artículos 270 y otros del Código Penal

Ø **Falsedades,** Artículos 386 y ss. del Código Penal

Ø **Sabotajes informáticos.**

Delito de daños mediante la destrucción o alteración de datos, programas o documentos electrónicos contenidos en redes o sistemas informáticos. (Artículo 263 y otros del Código Penal)

Ø **Fraudes informáticos.**

Delitos de estafa a través de la manipulación de datos o programas para la obtención de un lucro ilícito. (Artículos 248 y ss. del Código Penal)

Ø **Amenazas.**

Realizadas por cualquier medio de comunicación. (Artículos 169 y ss. del Código Penal)

Ø **Calumnias e injurias.**

Cuando se propaguen por cualquier medio de eficacia semejante a la imprenta o la radiodifusión. (Artículos 205 y ss. del Código Penal)

Ø **Pornografía infantil.**

Entre los delitos relativos a la prostitución al utilizar a menores o incapaces con fines exhibicionistas o pornográficos.

- La inducción, promoción, favorecimiento o facilitamiento de la prostitución de una persona menor de edad o incapaz. (art. 187)

- La producción, venta, distribución, exhibición, por cualquier medio, de material pornográfico en cuya elaboración hayan sido utilizados menores de edad o incapaces, aunque el material tuviere su origen en el extranjero o fuere desconocido. (art. 189)

- El facilitamiento de las conductas anteriores (*El que facilitare la producción, venta, distribución, exhibición.***). (art. 189)**

- La posesión de dicho material para la realización de dichas conductas. (art. 189)

Perú

Ley N° 27.309, promulgada el 15 de julio de 2000 y publicada el 17 de julio de 2000, incorporó los

delitos informáticos al Código Penal.

CAPÍTULO X.

DELITOS INFORMÁTICOS.

Artículo 207º-A. El que utiliza o ingresa indebidamente a una base de datos, sistema o red de computadoras o cualquier parte de la misma, para diseñar, ejecutar o alterar un esquema u otro similar, o para interferir, interceptar, acceder o copiar información en tránsito o contenida en una base de datos, será reprimido con pena privativa de libertad no mayor de dos años o con prestación de servicios comunitarios de cincuenta y dos a ciento cuatro jornadas.

Si el agente actuó con el fin de obtener un beneficio económico, será reprimido con pena privativa de libertad no mayor de tres años o con prestación de servicios comunitarios no menor de ciento cuatro jornadas.

Artículo 207º-B. El que utiliza, ingresa o interfiere indebidamente una base de datos, sistema, red o programa de computadoras o cualquier parte de la misma con el fin de alterarlos, dañarlos o destruirlos, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años y con setenta a noventa días multa.

Artículo 207º-C. En los casos de los artículos 207º-A y 207º- B, la pena será privativa de libertad no menor de cinco ni mayor de siete años, cuando:

1. El agente accede a una base de datos, sistema o red de computadora,
haciendo uso de información privilegiada, obtenida en función a su cargo.
2. El agente pone en peligro la seguridad nacional.

5.- ANTECEDENTES DE LA PROBLEMÁTICA INTERNACIONAL

5.1.- ACCIONES REALIZADAS POR LA COMUNIDAD INTERNACIONAL PARA LA PREVENCIÓN Y CONTROL FORMAL E INFORMAL DEL CIBERCRIMEN.

5.1.1.- ORGANIZACIÓN DE LAS NACIONES UNIDAS

TIPOS DE DELITOS INFORMÁTICOS RECONOCIDOS POR NACIONES UNIDAS

5.1.1.1.- Fraudes cometidos mediante manipulación de computadoras

Ø 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.

Ø 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 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.

Ø 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 basándose en 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.

Ø 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.

5.1.1.2.- **Falsificaciones informáticas**

Ø COMO OBJETO

Cuando se alteran datos de los documentos almacenados en forma computarizada.

Ø COMO INSTRUMENTOS

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

5.1.1.3.- Daños o modificaciones de programas o datos computarizados

Ø 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:

Ø Virus

Es una serie de claves programáticas que pueden adherirse a los programas legítimos y propagarse a otros programas informáticos. Un virus puede ingresar en un sistema por conducto de una pieza legítima de soporte lógico que ha quedado infectada, así como utilizando el método del Caballo de Troya o por medio de la transmisión de datos vía correo electrónico, reenviadles y ejecutables.

Ø 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.

Ø 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

5.1.1.4.- 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.

Ø 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.

5.1.1.5.- 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, se considera, 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.

5.1.2.- UNION EUROPEA:

La Comunidad Europea, en los cursos de acción desarrollados para la prevención y control de delitos informáticos ha generado una importante gama de políticas, en el ámbito judicial, político y policial, dando como principio el que Europa se ha caracterizado por pasar de una sociedad industrial a la sociedad de la información, esto ha dado grandes progresos en todos los aspectos de la vida humana: el trabajo, la educación y el ocio, el gobierno, la industria y el comercio. Las nuevas tecnologías de información y comunicación están teniendo un impacto revolucionario y fundamental en nuestras sus economías y sociedades. Consideran que el éxito de la sociedad de la información es importante para el crecimiento, la competitividad y las posibilidades de empleo de Europa, y tiene repercusiones económicas, sociales y jurídicas de gran envergadura.

Para el logro de estos objetivos de crecimiento, competitividad y posibilitar la creación de nuevos empleos, se han volcado en las siguientes actividades legislativas. En diciembre de 1999, la Comisión puso en marcha la iniciativa eEuropa , con el fin de garantizar que Europa se beneficie de las tecnologías digitales, y que la nueva sociedad de la información sea socialmente inclusiva. En junio de 2000, el Consejo Europeo de Feira, adoptó el Plan de acción eEuropa, y solicitó que se aplicara antes de finales de 2002. El plan de acción resalta la importancia de la seguridad de las redes y de la lucha contra la delincuencia informática, en atención a que las infraestructuras de información y comunicación se ha convertido en una parte crucial de las economías de los países miembros de la Comunidad.

La Unión Europea ha tomado ya diversas medidas para luchar contra los contenidos ilícitos y nocivos en Internet, para proteger la propiedad intelectual y los datos personales, para promover el comercio electrónico y el uso de la firma electrónica y para aumentar la seguridad de las transacciones. En abril de 1998, la Comisión presentó al Consejo los resultados de un estudio sobre la delincuencia informática, llamado estudio “COMCRIME”. En octubre de 1999, la cumbre de Tampere del Consejo Europeo concluyó que la labor para acordar definiciones y sanciones comunes debe incluir la delincuencia de alta tecnología. El Parlamento Europeo también realizó un llamamiento para que se establezcan definiciones comúnmente aceptables de los delitos informáticos y se aproximen las legislaciones, en especial en el ámbito del derecho penal. El Consejo de la Unión Europea ha adoptado una posición común respecto a las negociaciones del Convenio del Consejo de Europa sobre delincuencia en el ciberespacio y ha adoptado varios elementos iniciales como parte de la estrategia de la Unión contra la delincuencia de alta tecnología.

Algunos Estados miembros de la UE también han estado en la vanguardia de las actividades del G8 a este respecto. La presente Comunicación trata la necesidad y las posibles formas de una iniciativa política amplia en el contexto de los objetivos más amplios de la sociedad de la información y de la libertad, seguridad y justicia, con el fin de mejorar la seguridad de las infraestructuras de información y luchar contra la delincuencia informática, de acuerdo con el compromiso de la Unión Europea de respetar los derechos humanos fundamentales. (Carta de los Derechos Fundamentales de la UE)

En el corto plazo, la Comisión opina que existe una clara necesidad de un instrumento de que la UE garantice que los Estados miembros dispongan de sanciones efectivas para luchar contra la pornografía infantil en Internet. La Comisión presentará a finales del presente año una propuesta de decisión marco que, en un contexto más amplio, abarcará cuestiones asociadas con la explotación sexual de los niños y el tráfico de seres humanos, incluirá disposiciones para la aproximación de leyes y sanciones.

A más largo plazo, la Comisión presentará propuestas legislativas para seguir aproximando el derecho penal sustantivo en el ámbito de la delincuencia de alta tecnología. De acuerdo con las conclusiones del Consejo Europeo de Tampere de octubre de 1999, la Comisión considerará asimismo las opciones del reconocimiento mutuo de los autos anteriores al juicio, asociados con las investigaciones de delitos informáticos.

Paralelamente, la Comisión se propone promover la creación, donde no exista, de unidades de policía especializadas en delincuencia informática a escala nacional; apoyar la formación técnica pertinente para la aplicación de la ley; y fomentar las acciones europeas tendientes a la seguridad de la información.

En el plano técnico, y en línea con el marco jurídico, la Comisión promoverá el Desarrollo Informático, para comprender y reducir los puntos vulnerables, estimulará la difusión de conocimientos técnicos.

La Comisión se propuso también crear un foro comunitario que reúna a los organismos competentes, a los proveedores de servicios de Internet, a los operadores de telecomunicaciones, a las organizaciones de libertades civiles, a los representantes de los consumidores, a las autoridades responsables de la protección de datos y a otras partes interesadas, con el objetivo de aumentar la comprensión y la cooperación mutuas a escala de la UE. El foro intentará aumentar la conciencia pública de los riesgos que presentan los delincuentes en Internet, promover las mejores prácticas para la seguridad, determinar instrumentos y procedimientos eficaces para luchar contra la delincuencia informática y fomentar el desarrollo futuro de mecanismos de detección temprana y gestión de crisis.

La delincuencia informática se comete en el ciberespacio, y no se detiene en las fronteras nacionales convencionales. En principio, puede perpetrarse desde cualquier lugar y contra cualquier usuario de ordenador del mundo. Se necesita una acción eficaz, tanto en el ámbito nacional como internacional, para luchar contra la delincuencia informática. Plan de Acción e-Europa.

A escala nacional, en muchos casos no hay respuestas globales y con vocación internacional frente a los nuevos retos de la seguridad de la red y la delincuencia informática. En la mayoría de los países, las reacciones frente a la delincuencia informática se centran en el derecho nacional (especialmente el derecho penal), descuidando medidas alternativas de prevención.

La Directiva 2000/31/CE, sobre el comercio electrónico modifica esto por lo que se refiere a la responsabilidad de los proveedores de servicios intermediarios sobre determinadas actividades intermediarias. Asimismo, la Directiva prohíbe a los Estados miembros imponer a los proveedores de servicios intermediarios una obligación general de supervisar los datos que transmitan o almacenen.

Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico).

A escala internacional y supranacional, se ha reconocido ampliamente la necesidad de luchar eficazmente contra la delincuencia informática, y diversas organizaciones han coordinado o han intentado armonizar actividades al respecto. Los Ministros de Justicia y de Interior del G8 adoptaron en diciembre de 1997 un conjunto de principios y un plan de acción de 10 puntos, que fue aprobado por la Cumbre del G8 en Birmingham en junio de 1998 y que se aplica en la actualidad. El Consejo de Europa comenzó a elaborar un convenio internacional sobre la delincuencia cibernética en febrero de 1997 y se espera que acabe esta tarea el presente año. La lucha contra la delincuencia cibernética también figura en el orden del día de las discusiones bilaterales que la Comisión Europea celebra con algunos gobiernos (de fuera de la UE). Se ha creado un grupo de trabajo conjunto CE/EE.UU. sobre protección de infraestructuras críticas.

El Consejo JAI de la UE de 19 de marzo de 1998 aprobó los 10 principios para combatir la delincuencia de alta tecnología adoptados por el G8, e invitó a los Estados miembros de la UE no pertenecientes al G8 a unirse a la red.

Bajo los auspicios del grupo consultivo conjunto del Acuerdo de cooperación científica y tecnológica celebrado entre la UE y EE.UU. La ONU y la OCDE también han estado activas en este ámbito, y se está discutiendo en foros internacionales como el Diálogo Empresarial Global y el Diálogo Empresarial Transatlántico.

Naciones Unidas elaboró un "Manual sobre la prevención y el control de la delincuencia informática", que se ha actualizado recientemente. En 1983, la OCDE inició un estudio sobre la posibilidad de aplicar a escala internacional y armonizar los derechos penales para abordar el problema del abuso informático o de la delincuencia informática. En 1986, publicó el informe "Delincuencia informática: Análisis de las medidas jurídicas", donde se examinaban las leyes y propuestas existentes para la reforma en varios Estados miembros y se recomendaba una lista mínima de abusos que los países deberían prohibir y penalizar con leyes penales, en 1992, la OCDE elaboró un conjunto de directrices para la seguridad de los sistemas de información, que deberían en principio proporcionar una base sobre la cual los Estados y el sector privado pudieran construir un marco para la seguridad de los sistemas de información.

Hasta hace poco, la acción legislativa en la Unión Europea ha adoptado básicamente la forma de medidas en los ámbitos de los derechos de autor, la protección del derecho fundamental a la intimidad y la protección de datos, los servicios de acceso condicional, el comercio electrónico, la firma electrónica y en especial la liberalización del comercio de productos de cifrado, que están relacionados de forma indirecta con la delincuencia informática.

También se han adoptado varias medidas no legislativas importantes en los últimos 3 o 4 años. Entre éstas figuran el plan de acción contra los contenidos ilícitos y nocivos en Internet, que co-financia acciones de concienciación, experimentos de clasificación y filtrado de contenidos y líneas directas, e iniciativas relativas a la protección de menores y de la dignidad humana en la sociedad de la información, la pornografía infantil y la interceptación legal de las comunicaciones. La UE ha apoyado durante mucho tiempo proyectos tendientes a promover la seguridad y la confianza en infraestructuras de información y transacciones electrónicas, y recientemente ha aumentado la dotación del presupuesto del programa asociado TSI. También se han apoyado proyectos operativos y de investigación dirigidos a promover la formación especializada de las autoridades competentes, así como la cooperación entre estas autoridades y el sector en cuestión, en el marco de programas del tercer pilar tales como STOP, FALCONE, OISIN y GROTIUS.

Recomendación 98/560/CE del Consejo de 24 de septiembre de 1998 relativa al desarrollo de la competitividad de la industria europea de servicios audiovisuales y de información mediante la promoción de marcos nacionales destinados a lograr un nivel de protección comparable y efectivo de los menores y de la dignidad humana;

El plan de acción para luchar contra la delincuencia organizada, adoptado por el Consejo JAI en mayo de 1997 y aprobado por el Consejo Europeo de Amsterdam, incluía una petición para que la Comisión elaborase, para finales de 1998, un estudio sobre la delincuencia informática. Este estudio, llamado 'estudio COMCRIME', fue presentado por la Comisión al grupo de trabajo multidisciplinar del Consejo contra la delincuencia organizada en abril de 1998. La presente Comunicación es en parte una respuesta a la petición del Consejo JAI.

"Aspectos jurídicos de la delincuencia informática en la sociedad de la información - COMCRIME". El estudio fue elaborado por el profesor U. Sieber de la Universidad de Würzburg, en virtud de un contrato con la Comisión Europea.

Antes de elaborar esta Comunicación, la Comisión consideró apropiado realizar consultas informales con representantes de las autoridades competentes de los Estados miembros y de las autoridades de control de la protección de datos, así como de la industria europea (especialmente PSI y operadores de telecomunicaciones).

El Programa de Tecnologías de la Sociedad de la Información de la UE (TSI), en especial los trabajos relativos a la información, la seguridad de la red, y otras tecnologías dirigidas a crear seguridad, proporcionan un marco para desarrollar la capacidad y la tecnología para comprender y abordar nuevos retos relacionados con la delincuencia informática. Estas tecnologías incluyen herramientas técnicas para la protección contra la violación de los derechos fundamentales a la intimidad y los datos personales y otros derechos personales, y para la lucha contra la delincuencia informática. Además, en el contexto del Programa TSI, se ha puesto en marcha una iniciativa de seguridad. Esta iniciativa contribuirá a la seguridad y a la confianza en infraestructuras de información muy interconectadas y en sistemas de alta integración en redes, promoviendo la toma de conciencia respecto a la seguridad y las tecnologías que proporcionan seguridad. Parte integrante de esta iniciativa es la cooperación internacional. El Programa TSI ha desarrollado relaciones de trabajo con la Agencia de Proyectos de Investigación Avanzada para la Defensa (DARPA) y la Fundación Nacional para la Ciencia (NSF), y ha establecido, en colaboración con el Departamento de Estado de EE.UU., un grupo de trabajo conjunto CE/EE.UU. sobre protección de infraestructuras críticas .

El programa TSI, lo gestiona la Comisión Europea. Forma parte del 5º Programa Marco 1998-2002. Bajo los auspicios del Grupo consultivo conjunto del Acuerdo de cooperación científica y tecnológica firmado entre la UE y EE.UU.

Por último, el establecimiento de obligaciones relativas a la seguridad, derivadas en particular de las Directivas comunitarias sobre protección de datos, contribuye a mejorar la seguridad de las redes y del procesamiento de datos.

Ø Unidades especializadas a escala nacional.

Dada la complejidad técnica y jurídica de algunos delitos informáticos, la Comunidad Europea ha dado importancia a la creación de unidades especializadas a escala nacional. Tales unidades especializadas,

compuestas por personal pluridisciplinar (policial y judicial) y con grandes conocimientos, deberían contar con instalaciones técnicas adecuadas y funcionar como puntos de contacto rápidos con los siguientes fines:

· responder rápidamente a las solicitudes de información sobre presuntos delitos. Para ello ha definido formatos comunes para el intercambio de tal información, aunque los debates de los expertos del G8 han puesto de manifiesto que esto puede no ser tarea fácil, dadas las diferencias entre las culturas jurídicas nacionales;

· Actuar como interfaz de las autoridades competentes, nacional e internacionalmente, para las líneas directas, recibiendo denuncias de los usuarios de Internet sobre contenidos ilícitos; hasta ahora, sólo existen líneas directas en unos pocos países. Los ejemplos son Cybertipline en EE.UU. e Internet Watch Foundation (IWF) en el Reino Unido, que desde diciembre de 1996, gestiona una línea directa de teléfono y de correo electrónico para que el público informe acerca del material encontrado en Internet que consideren ilícito. La IWF juzga si el material es ilícito, informa a los PSI y a la policía. También existen otros organismos de supervisión en Noruega (Redd Barna), Países Bajos (Meldpunt), Alemania (Newswatch, FSM y Jugendschutz), Austria (ISPAA) e Irlanda (ISPAI). En el marco del programa comunitario Daphne, Childnet International ha iniciado recientemente un proyecto relacionado directamente con esta cuestión ("Foro internacional de proveedores de líneas directas en Europa"). La reunión de expertos de la UNESCO en París en enero de 1999 apoya y fomenta también las líneas directas nacionales y la creación de redes de líneas directas, o de una "atalaya electrónica" internacional.

· Mejorar o desarrollar técnicas especializadas de investigación informática con el fin de detectar, investigar y procesar delitos informáticos;

· actuar como centro de excelencia en cuestiones relacionadas con la delincuencia cibernética, con el fin de compartir experiencias y mejores prácticas.

En la UE, algunos Estados miembros ya han creado estas unidades especializadas que tratan específicamente los delitos informáticos. La Comisión considera que la creación de tales unidades especializadas es una prerrogativa de los Estados miembros y anima a éstos a que tomen medidas en esa dirección. La compra del hardware y software más avanzado para estas unidades, así como la formación del personal, supone grandes costos y presupone prioridades y decisiones políticas en los niveles gubernamentales correspondientes. La experiencia de unidades ya existentes en los Estados miembros puede ser particularmente valiosa.

La Comisión también opina que Europol puede proporcionar mayor valor añadido a escala de la UE mediante la coordinación, el análisis y otras ayudas a las unidades nacionales especializadas. Por tanto, la Comisión apoyará la ampliación del mandato de Europol para cubrir la delincuencia cibernética.

Ø Formación especializada: Se requiere un considerable esfuerzo en el ámbito de la formación continua y especializada del personal policial y judicial. Las técnicas y las capacidades de la delincuencia

informática evolucionan con más rapidez que las correspondientes a áreas más tradicionales de actividad delictiva.

Algunos Estados miembros han llevado a cabo iniciativas sobre formación en alta tecnología del personal responsable de la aplicación de la ley. Estos Estados están en condiciones de proporcionar asesoramiento y orientación a países ajenos a la Comunidad o Estados miembros que aún no han tomado medidas similares.

Ø Se han lanzado proyectos individuales tendentes a este fin, en forma de intercambio de experiencias y seminarios sobre los retos comunes a que se enfrentan los profesionales en cuestión, con el apoyo de programas gestionados por la Comisión (en especial STOP, FALCONE y GROTIUS). La Comisión propondrá más actividades en este campo, incluida la formación informática y en línea.

Ø Europol ha tomado la iniciativa de organizar una sesión de formación de una semana para el personal de los Estados miembros responsable de la aplicación de la ley, en noviembre de 2000, con especial referencia al problema de la pornografía infantil. El alcance de la sesión podría ampliarse para incluir la delincuencia informática en general. INTERPOL también permanece activa en este ámbito desde hace varios años. Sus iniciativas podrían ampliarse para incluir un mayor número de personal.

El G8 ha organizado iniciativas tendentes al intercambio de experiencias entre las autoridades competentes, y al establecimiento de técnicas comunes de investigación, basándose en casos concretos. Se espera que se adopte otra iniciativa en el ámbito de la formación en la segunda mitad de 2001. Los Estados miembros de la UE pertenecientes al G8 podrían compartir estas experiencias con los otros Estados miembros.

Ø En el ámbito específico de la lucha contra la pornografía infantil en Internet, la creación y el mantenimiento de una biblioteca central digital de imágenes de pornografía infantil a escala internacional (que estaría disponible en Internet para las unidades nacionales especializadas de policía, con las condiciones y limitaciones necesarias por lo que respecta al acceso y la protección de la intimidad), ayudaría a la búsqueda de víctimas y delincuentes, y contribuiría a determinar la naturaleza de los delitos y a formar a los funcionarios de policía especializados.

En este contexto, el proyecto "Excalibur", elaborado por la división nacional sueca de inteligencia sobre delincuencia y copatrocinado por la Comisión Europea bajo el programa STOP, ha sido una iniciativa muy acertada. Este proyecto se ha creado con la cooperación de las fuerzas de policía de Alemania, el Reino Unido, los Países Bajos y Bélgica, así como Europol e INTERPOL. También hay que considerar otros proyectos realizados por el BKA alemán ("Perkeo") y el Ministerio de interior francés (proyecto "Surfimage", también copatrocinado por el programa STOP).

Ø Mejor información y normas comunes sobre mantenimiento de archivos

La creación de un conjunto armonizado de normas sobre mantenimiento de archivos policiales y judiciales, y de instrumentos adecuados para el análisis estadístico de la delincuencia informática, ayudaría a las autoridades policiales y judiciales competentes a almacenar, analizar, y evaluar mejor la información recogida en este área cambiante.

Ø Asimismo, desde el punto de vista del sector privado, estas estadísticas son necesarias para la correcta evaluación de los riesgos y el análisis de costes y beneficios de su gestión. Esto es importante no sólo por razones operativas (como las decisiones acerca de las medidas de seguridad que deben tomarse), sino también a efectos del seguro.

Se está actualizando y haciendo accesible para la Comisión una base de datos sobre el estatuto de la delincuencia informática, que se presentó como parte del estudio COMCRIME. La Comisión estudiará la posibilidad de mejorar el contenido (inclusión de leyes y jurisprudencia) y la utilidad de la base de datos.

5.2.- RESPONSABILIDADES ENTREGADAS A LOS ORGANISMOS POLICIALES EXTRANJEROS

Ø **INTERPOL:**

La INTERPOL Internacional, a través de los últimos años se ha dedicado a la investigación de delitos y fraudes computacionales, ante lo cual participa en la creación de un organismo Internacional de cooperación con otros miembros de INTERPOL a través de Europa, África, Asia y América, dando origen a Crímenes de Tecnologías de la información (ITC: Information Technology Crime); abocadas a la investigación y persecución de los delitos de este tipo en todas las áreas del planeta que requieran cooperación.

Para ello, se ha editado el Manual del Crimen Computacional 2001.

http://www.interpol.com

Ø **FBI**

INTERNET FRAUD COMPLATION CENTER (FBI/NW3C)

El Servicio de Investigaciones de FBI, ante la creciente demanda de Instituciones, Empresas y Personas, afectadas por la acción de delitos informáticos se une en la implementación con el “Centro de Delitos de Cuello Blanco” (National White Collar Crime Center (NW3C)), a fin de realizar las acciones tendientes para la prevención y control de los fraudes y delitos informáticos, como preparación de documento

http://www.fbi.gov

Ø **CUERPO NACIONAL DE POLICIA ESPAÑOLA:**

UNIDAD DE INVESTIGACIÓN DE DELINCUENCIA EN TECNOLOGÍAS DE LA INFORMACIÓN:

La Unidad de Investigación de la Delincuencia en Tecnologías de la Información nace en el transcurso del año 2000 con el propósito de impulsar, coordinar y realizar investigaciones relacionadas con la criminalidad de las nuevas tecnologías y las comunicaciones en España, estrechar las relaciones con las demás policías de la Comunidad Europea. Dependiente del Ministerio del Interior del Reino de España.

http://www.mir.es/policia/

Ø **POLICIA NACIONAL DE LA REPUBLICA DE FRANCIA**

OFICINA CENTRAL DE LUCHA CONTRA LA CRIMINALIDAD LIGADA A LAS TECNOLOGIAS DE LA INFORMACIÓN Y LAS COMUNICACIONES.

A raíz de los altos requerimientos para la investigación de los ciberdelitos, el Primer Ministro Don Lionel Jospen, determina la creación de un organismo centralizado, estructurado y especializado en esta nuevas fuentes de información, ante lo cual, por decreto de fecha 15 de Mayo del 2000, entra en actividades la "**Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication (O.C.L.C.T.I.C.)**" con la finalidad de cooperar al servicio de judicatura, en las nuevas técnicas tecnológicas, cooperar y asistir al Poder Judicial en delitos de graves costos sociales. Haciéndose asesorar por expertos en todas las áreas de la informática, penal y social.

http://www.interieur.gouv.fr/police/oclctic/index.htm

6.- ANTECEDENTES DE LA PROBLEMÁTICA NACIONAL

6.1.- INFOESTRUCTURA PARA LA ECONOMÍA DIGITAL.

La sustitución de los mecanismos tradicionales para la realización de transacciones y trámites, por el uso de métodos intensivos en tecnologías de información, está dando origen a una nueva forma de actividad, llamado "la nueva economía digital", cuyos importantes beneficios en productividad, plantean nuevos desafíos de incorporar rápida y masivamente a los agentes económicos en la red. La no oportuna incorporación, llevará inevitablemente a la pérdida de oportunidades que ofrece el acceso a la información, como son mercados más amplios, menores costos de producción, mayor capacitación; como también pueden dar origen a la pérdida de posiciones privilegiadas alcanzadas en la economía tradicional, por esto las tecnologías de la

información (TI), se constituyen en un factor determinante del crecimiento y desarrollo económico, cuya insuficiencia significa el ensanchamiento de las brechas con los países que más rápidamente se incorporan a la economía digital.

Para el logro del objetivo de acelerar la velocidad de acceso y uso de Internet como herramienta de información, transacción y educación; el rol que al Estado le ha correspondido asumir en la nueva economía digital es:

Ø Promover el acceso universal a Internet.

Ø Eliminar las barreras que interfieren en el acceso y uso de las redes.

Ø Establecer las condiciones para el desarrollo de inversiones en los ámbitos de la infraestructura de soporte a la economía digital y de contenido.

Ø Velar por el desarrollo de recursos humanos compatibles con los requerimientos de la nueva

economía digital.

Ø Convertirse en un agente catalizador de uso de Internet, mediante la modernización del aparato público.

6.1.2.- TRANSACCIONES EN LA ECONOMIA DIGITAL

Es posible encontrar diferentes contenidos potenciales de ser transados a través de la red Internet, según sea el origen público o privado del oferente y según el destino del demandante, de esta manera las transacciones se han clasificado en la siguiente forma:

Ø E-governmet: representa las transacciones de servicios provistos por el Estado a la población y las empresas, los que pueden o no tener una contrapartida financiera, como por ejemplos son el trámite de pago de impuestos (Operación renta 2001, www.sii.cl), solicitud de antecedentes personales (www.registrocivil.cl), solicitud de hora para una consulta médica en un establecimiento del sector público.

Ø E-commerce: representa las transacciones comerciales para la adquisición de bienes y servicios de carácter privado, estas se clasifican, a su vez, según el destinatario de los bienes y servicios transados en:

- business to business, (b2b): refleja las transacciones de insumos entre empresas.

- Business to consumers: (b2c), refleja las transacciones de bienes y servicios entre empresas y consumidores.

Para el éxito de las transacciones a través de la red, se requieren de dos requisitos básicos:

Ø Infraestructura que permita el transporte de la información, haciendo posible el encuentro electrónico entre oferentes y demandantes, así como infraestructura de medios necesarios para que los acuerdos sean aceptados por las partes involucradas e infraestructura para el transporte de los bienes transados electrónicamente desde el oferente hasta el demandante.

Ø Contenido de información necesaria que permite a ambas partes, oferentes y demandantes, tanto del sector público, como privado, conocer adecuadamente los términos en los que los bienes y servicios son ofrecidos.

Al conjunto de infraestructura y contenido, se le ha denominado infoestructura. La ausencia o limitaciones de uno de los contenidos, no garantiza el éxito de las transacciones en la red.

Es por la imperiosa necesidad de lograr los sustentos para la infoestructura de la economía digital, que la Subsecretaria de Telecomunicaciones de Chile, en mayo del año 2000, emitió sus desafíos y prioridades, entre las que destacamos:

Ø Desarrollo eficiente de infraestructura de telecomunicaciones. Para garantizar el crecimiento sostenido y sustentable de la economía, se hace necesario la generación de condiciones para obtener un acelerado desarrollo de la infraestructura de información, para en el corto plazo lograr un significativo incremento de la productividad de la economía. La expansión de la capacidad y cobertura de las infraestructuras de telecomunicaciones, teniendo como meta el año 2006 todo el país se encuentre conectado a la red, desplazando las diferencias existentes actualmente hacia la superioridad de la Región Metropolitana.

Ø Eliminación de barreras a las transacciones electrónicas, considera el crecimiento sostenido y sustentable, mediante la eliminación de factores que impiden la mejor utilización de la TI, inhibiendo el comercio electrónico y otras actividades de negocios en la red.

Ø Incorporación del Estado en las redes, esto constituye un elemento catalizador de la economía digital, permitiendo al mismo tiempo mejorar la calidad de vida de los ciudadanos, acercándose los servicios públicos a sus usuarios.

Ø Construcción de infoestructura para los sectores más vulnerables y/o marginados, esto con la finalidad de avanzar con igualdad, mejorando el acceso a las oportunidades y la calidad de vida de la población; ya que con ella los grupos tradicionalmente más marginados de las oportunidades pueden disfrutar del bienestar que alcance el resto de la sociedad, especialmente en áreas como la rural, la discapacidad o la pobreza urbana dejan de constituir limitantes del desarrollo de las comunidades.

Ø Facilitar la incorporación de la radiofusión y de otras redes tradicionales como proveedores de infoestructura.

Ø Fortalecimiento de los derechos de los usuarios y corrección de las distorsiones que pueden existir en el mercado de la infraestructura, a fin de asegurar condiciones competitivas, esto por medio de la organización de un sistema de protección para la competencia, los consumidores y los usuarios, asegurando un acceso seguro a las telecomunicaciones, en condiciones justas de precios y calidad.

6.2.- ECONOMIA DIGITAL

6.2.1- Beneficios de la Revolución Tecnológica

Las Tecnologías de la Información (TI) están redefiniendo conductas que regulan la interacción social: para ciertos propósitos, el tiempo y el espacio han dejado de ser dimensiones restrictivas en el actuar de las personas, las empresas y los gobiernos. Las TI están revolucionando la actividad económica mundial con un alcance sin precedentes, en la totalidad de los sectores productivos y en especial en aquellos que utilizan en forma más intensiva la información. Las TI apuntan hacia la optimización del uso de los recursos en las empresas, así como al interior de los mercados, induciendo aumentos de eficiencia en los servicios al cliente interno y externo.

Todo esto apoyado en las potencialidades implícitas de las TI en el ámbito de la generación, procesamiento y distribución de la información.

Los beneficios asociados a esta revolución tecnológica han producido un efecto importante en la demanda de TI tanto en Chile como en el resto del mundo. Aunque Chile tiene una participación pequeña en este gasto (en torno al 1%), durante la última década se han registrado incrementos significativos en las inversiones en esta área. En 1985 se gastaron US $132 millones en TI y en el año 2000, US $1.138 millones, reflejando un crecimiento anual promedio de 16%.

6.2.2.- Evolución de las Tecnologías de la Información en Chile

Entre 1985 y el año 2000, la participación del gasto en TI sobre el producto se ha más que duplicado, pasando de 0,8% A 1,7%. Si bien estas cifras podrían apresurar algunas conclusiones conformistas en cuanto a que Chile habría realizado una “buena” labor en términos de expansión del gasto en TI, la experiencia de otros países hace perder relevancia al liderazgo tecnológico de Chile en la región latinoamericana. Ya a comienzos de los noventa, algunos países no necesariamente industrializados avizoraron con mayor claridad y profundidad el rol que jugarían las TI en los procesos de desarrollo, y emprendieron una ardua carrera en pos de la inserción social en el mundo informatizado. Chile, en cambio, viene presenciando una desaceleración en las tasas de crecimiento de la inversión en TI, situación que ha incidido en la pérdida del liderazgo tecnológico que el país ostentó frente a la comunidad regional.

6.2.3.- Naturaleza de la Brecha Digital

Si bien Internet, tiene la capacidad de tender a igualar oportunidades entre personas, empresas y países, existe un período inicial de alto riesgo en que los primeros que acceden a la innovación tecnológica -y se benefician de ella- son quienes tienen mayor poder económico y se encuentran más cercanos a la generación y difusión del cambio tecnológico.

Durante este período de riesgo, la brecha económica entre los aventajados y el resto tiende a aumentar, debido a que los primeros mejoran su posición relativa al hacer uso de las nuevas técnicas. Si bien la impresionante velocidad de propagación de Internet tiende a mitigar los desequilibrios con el tiempo, la duración de ese período de ensanchamiento de la brecha puede llegar a constituir un serio peligro para los menos adelantados, amenazando, en el caso de las empresas, su viabilidad económica.

A nivel mundial, la brecha entre los países desarrollados y en desarrollo se ha ampliado en los últimos años, debido en gran parte a la masificación del uso de las tecnologías de información en Norteamérica, Europa y Japón. En conjunto, los países pobres y en desarrollo albergan al 85% de la población mundial, pero sólo generan la quinta parte del PIB. Esta disparidad es lo que se conoce como la brecha económica.

Lo anterior se encuentra estrechamente relacionado con el proceso de innovación tecnológica. Cada vez que surge una nueva innovación, debido a que los países más avanzados son los primeros (o los únicos) en adoptarla, los beneficios derivados de su uso aceleran su crecimiento económico, ampliando la brecha que mantienen con los países en desarrollo.

En el caso de la revolución de las TI, inicialmente se ha producido una brecha digital entre los países desarrollados y en desarrollo. Como se mencionó, los países en desarrollo concentran el 85% de la población y generan sólo el 21% del PIB. En materia de TI, apenas tienen el 8% de la población Internet y realizan el 4% del comercio electrónico mundial.

6.2.4.- La Brecha Digital en Chile

En el caso de Chile, se observa la replicación de esta misma tendencia. La Nueva Economía no es una posibilidad inmediata para la totalidad de los chilenos, ni para el conjunto de las empresas del país. La información confirma una significativa inequidad en el acceso a la red, tanto desde el punto de vista de los distintos segmentos empresariales, como de los estratos socioeconómicos y de su distribución geográfica a lo largo del territorio nacional.

La ciudad capital, Santiago, concentra el 57% de las líneas telefónicas fijas y el 58% de los aparatos telefónicos móviles. La tele-densidad fija en la Región Metropolitana está 9 puntos por sobre el índice nacional (20 líneas por cada 100 habitantes), y sólo las regiones XII, V y II exhiben niveles comparables, mientras que aquellas con un alto nivel de población rural, como la VI y la VII, cuentan con menos de la mitad. Esto se traduce en el claro predominio de la Región Metropolitana en materia de conexiones a Internet (57% del total) y de las transacciones realizadas por este medio, que superan el 70%. Ello, pese a que el 60% de la población nacional vive en regiones, donde además se genera el 52% del PIB.

6.3.- La Seguridad Informática en la Economía Digital

Durante los últimos años, se ha hace cada vez más evidente una creciente preocupación sobre los niveles reales de seguridad que detentan los sistemas informáticos de empresas, agencias de gobierno y personas naturales.

Las más recientes inversiones en esta área han estado lideradas por la implementación de tecnologías que otorgan seguridad al comercio electrónico, en la medida en que una gran masa de empresas ha dirigido sus políticas de negocios hacia Internet, dado los fuertes beneficios potenciales que dicha tecnología otorga. La seguridad de las transacciones electrónicas pasó a ser un paso ineludible para impulsar y masificar los negocios a través de red.

Una serie de otros tópicos han preocupado a las empresas desde hace varios años destacándose fuertes inversiones en diversas áreas abarcando desde la protección de secretos industriales y el acceso restringido a los sistemas mediante el uso de claves, hasta la protección antivirus.

Si bien los problemas de seguridad de los sistemas informáticos han existido de hace mucho tiempo, los riesgos estaban medianamente controlados. Con el surgimiento de Internet apareció un conjunto numeroso de nuevos problemas de seguridad, profundizándose adicionalmente los ya existentes.

6.3.1. -Brechas de Seguridad en la Empresa

Una manera de medir el estado actual de la seguridad informática es visualizar la preocupación de las empresas a través de sus presupuestos en el área. Una encuesta realizada por la revista Information Security dio cuenta que los presupuestos en seguridad de las empresas, principalmente norteamericanas, se ha estado incrementado durante el último tiempo. Para lo anterior se realizó una comparación entre las empresas que gastan cantidades menores a los US$ 50 mil al año y las que gastan anualmente más de

US$ 1 millón. Del total de la muestra analizada, el número de compañías que gasta más de un millón de dólares se ha incrementado desde un 8% en 1998 hasta el 23% año 2000. A su vez el numero de compañías que gastan menos de 50 mil dólares al año en éste tema se ha reducido desde 52% a 23% en el mismo período.

Los sectores industriales más intensivos en recursos de seguridad (con excepción del área propia de la seguridad informática), han sido aquellos que por sus características requieren de la existencia de altos estándares de seguridad para asegurar la subsistencia de la industria. Dentro de éstos sectores, destacan el sector bancario y los servicios financieros, así como las firmas de alta tecnología, teniendo éstos los más altos presupuestos durante el año 2000. Por el contrario, las agencias gubernamentales, las universidades y las instituciones de salud son las que han tenido los más bajos gastos en el tema.

La principal preocupación del área de seguridad informática está centrada en los ataques de virus, en la pérdida de privacidad, la disponibilidad del servicio, y la explotación de las debilidades del hardware y del sistema operativo. A su vez, durante el año 2000 los principales proyectos de las empresas estuvieron dirigidos a otorgar seguridad en la red y las operaciones de comercio electrónico, seguidas el despliegue de mecanismos que previenen la intrusión externa de los sistemas informáticos.

Diversos estudios, dan cuenta que las causas de los problemas de seguridad de las compañías proviene principalmente de orígenes internos, por sobre las causas externas. Dentro de las primeras destacan algunas de uso generalizado, como la instalación de software no autorizado, y la infección de los equipos de la empresa por virus. Otros quiebres de seguridad suelen ser menos comunes, pero sus efectos pueden ser más dañinos, entre se encuentra la destrucción o divulgación malintencionada de información confidencial o simplemente el fraude.

Dentro de las brechas de origen externo, las más comunes, por lejos, son los virus, seguidos de la negación de servicio y un conjunto de ataques destinados a dañar distintas partes de los sistemas informáticos.

6.4.- BRECHAS DE SEGURIDAD

6.4.1.-Certificación Electrónica en Chile

La existencia de Autoridades Certificadoras (ACs) en Chile, constituye un fenómeno reciente que se inicia durante el año 2000 con el surgimiento de las primeras entidades administradoras de servicios de certificación.

En general, las ACs se originan como consecuencia de la masificación de Internet, fenómeno que ha

producido una creciente exposición de empresas y personas a riesgos de violaciones de seguridad.

En Latinoamérica y en Chile la adopción de tecnologías de certificación ha sido lenta, principalmente por la penetración y masificación de la red Internet.

En primer lugar, si bien es cierto la penetración de Internet ha crecido sistemáticamente, este incremento todavía no ha sido suficiente para generar una masa crítica de transacciones electrónicas que demande una gran cantidad de certificados y en segundo lugar, de los conectados a la red sólo un porcentaje menor realiza transacciones comerciales. Aún cuando uno de los motivos para este tipo de comportamiento es el temor al fraude, gran parte de esta conducta se da más bien por razones culturales, relacionadas a la dificultad para que las empresas y las personas cambien sus hábitos de compra y de negocios, en tercer lugar, existe un gran desconocimiento de los usuarios acerca de los riesgos reales involucrados en las transacciones electrónicas por medios inseguros.

Normalmente, en el mejor de los casos, se está consciente del más conocido de los fraudes, el robo del número de la tarjeta de crédito, motivo por el cual algunos usuarios evitan la compra en línea. Sin embargo, existen muchos otros riesgos de seguridad que habitualmente los usuarios desconocen, como la suplantación de personas, empresas, sitios Web, y la violación de los correos electrónicos.

En cuarto lugar, hasta la primera mitad de 2001 la actividad de certificación en Chile se desarrolló en ausencia de una legislación respecto de la validez de la firma digital y el contrato electrónico.

6.4.2.- Modelo Operacional de Certificación Electrónica en Chile

El modelo chileno de certificación, define a la Subsecretaría de Economía como el órgano rector que actúa como Entidad Acreditadora. A continuación se encuentra la Autoridad Certificadora, que es la entidad prestadora de servicios de certificación de firmas electrónicas autorizada, que da fe sobre los datos referidos a una firma electrónica a través del Acto Presencial por el cual cada persona o empresa debe atender. Finalmente se definen las Entidades de Registro, que actúan como organizaciones que representan a la Autoridad Certificadora en el trámite presencial que debe completar el solicitante de un certificado digital.

A comienzos de 2000, antes de la promulgación de la Ley de Firma Digital, algunos organismos pioneros ya estaban trabajando con firma digital o habían normado su uso dentro de sus respectivas comunidades, entre las que se encontraban el Servicio de Impuestos Internos, la Superintendencias de AFP´s, a través de Previred, la Superintendencia de Valores y Seguros, las Cajas de Compensación, y el Instituto de Normalización Previsional.

6.4.3. - Principales usos de la Certificación

En lo más simple, un certificado digital no es más que el equivalente electrónico de un carné de identidad, que permite identificar al suscriptor propietario.

La firma electrónica es el equivalente digital de la firma en papel, a través de la cual se establece la identidad del suscriptor de un determinado documento. A través de la certificación digital se cumplen 4 requerimientos con los que es posible obtener gran seguridad en todo tipo de transacciones electrónicas, evitando cualquier tipo de fraude. Ellos son:

a) Autentificación: Garantiza que las partes implicadas en la comunicación son realmente quienes dicen ser.

b) Confidencialidad: Garantiza que ninguna persona ajena a la comunicación puede tener acceso a la información enviada o recibida.

c) Integridad: Garantiza que los datos enviados deben ser exactamente iguales que los recibidos, sin que puedan ser manipulados por el receptor una vez terminada la comunicación.

d) No repudio: Garantiza que ninguno de los implicados en la transacción puede negar haber participado en ella.

Al mismo tiempo, se identifican 6 modalidades de uso frecuente para certificados digitales.

a) Identificación de personas para controlar los accesos a sitios Web restringidos o a determinados servicios en línea. En este caso puede ser una comunidad cerrada en la cual una empresa permite a determinadas personas acceder al sitio Web para manejar información restringida. Ese acceso se puede definir y asegurar a través del certificado digital.

b) Transacciones electrónicas. Ejemplo de ello pueden ser los bancos cuando solicitan a cada cuenta cuentacorrentista su identificación, cada vez que se genera una interacción del cliente con el sitio del banco, para efectuar movimientos en su cuenta corriente. Si el cliente tiene certificado digital y el sitio del banco también está certificado, la transacción se produce en un ambiente absolutamente seguro.

c) Trámites fiscales. En la Operación Renta 2001, los contribuyentes pudieron hacer su declaración de impuestos vía Internet autentificándose frente al sitio del Servicio de Impuestos Internos con certificados digitales. De este modo, se generó un entorno seguro para la transmisión de la información.

d) Intercambio de correo o e-mail seguro. Una de las actividades masivas que actualmente ocurren en la comunicación de personas y empresas es el uso del e-mail. En este canal, susceptible a intrusiones, el uso de certificado digital permite firmar el correo, identificando a quien emite y a quien se dirige la

comunicación, y también encriptar el contenido, haciéndolo extraordinariamente difícil de “hackear”.

e) La firma digital en documentos electrónicos, permite signar electrónicamente un Contrato, Orden de Compra u otro documento. A la luz de la Ley de Firma Digital, dichos actos celebrados por personas naturales o jurídicas, públicas o privadas, serán válidos y producirán los mismos efectos que los celebrados por escrito y en soporte de papel.

f) La Seguridad en Servidores Web permite a quien contacte un sitio certificado, tener la certeza de que se trata de ese sitio y no una suplantación, permitiendo realizar transacciones en forma segura.

6.5.- Proyecciones del Comercio Electrónico en Chile

6.5.1.- Comercio Electrónico Empresas – Personas (B2C)

Durante el año 2000, el acceso a Internet en Chile alcanzó al 9% de la población, proporcionalmente la tasa más alta de Latinoamérica. Entre los factores que explican la mayor penetración en el mercado local se encuentra el progresivo descenso en los costos de acceso, la mayor exposición comunicacional del fenómeno Internet, el surgimiento de contenidos locales y la mayor conectividad a nivel de empresas.

El número de usuarios promedió 1,4 millones de personas durante 2000, alcanzando a los 1,8 millones en diciembre. En dos años, la cantidad de internautas creció 10 veces.

Del total de usuarios, se estima que poco más del 10 por ciento realiza regularmente compras en Internet, lo que equivale a unas 175 mil personas. El promedio de compras entre los ciberconsumidores supera levemente los US$ 200 al año, nivel que se ubica por debajo de los estándares de países más desarrollados.

Las compras totales de los consumidores chilenos en Internet (B2C) alcanzaron a US$ 35,7 millones en 2000, registrando un aumento del 184% respecto del año anterior. La emergente oferta de e-tailers locales registró ventas por US$ 20,4 millones, equivalentes al 57% del total. Esta participación se ha dado en un contexto creciente, considerando que prácticamente el 100% de las ventas en 1998 (US$ 1,4 millones) correspondieron a importaciones desde sitios norteamericanos. El número de sitios chilenos de comercio electrónico detallista creció prácticamente diez veces entre septiembre de 1999 y marzo de 2000, totalizando más de 260 proveedores con una oferta total superior a los 340 mil productos.

Para el año 2001, se preveé un gasto total de US$ 74 millones en el segmento B2C, US$ 45 millones de los cuales corresponderían a ventas de sitios locales. Estas cifras superan las obtenidas en 2000, luego de lo cual darán paso a una desaceleración de la expansión del segmento, aún cuando se mantendrán elevadas tasas de crecimiento en el mediano plazo. Ello permitirá a los proveedores locales alcanzar ventas cercanas a los US$ 350 millones en el año 2005, sobre un total de US$ 500 millones para el segmento.

6.6.- Proyecciones del Comercio Electrónico en Chile

6.6.1.- Comercio Electrónico Empresas – Personas (B2C)

Los negocios entre empresas se han constituido en el eje transaccional del comercio electrónico en Chile. A partir de mediados de 2000 se ha producido un acelerado desarrollo de plataformas B2B, tanto abiertas como cerradas, que han dado origen a una mayor penetración del uso comercial de Internet en el segmento. De acuerdo a encuestas de la Cámara de Comercio de Santiago, en marzo de 2001 el 61% de las empresas contaba con alguna forma de acceso a Internet, y el 11% había desarrollado sus propios sitios Web.

El uso transaccional de la red por parte de las empresas, en tanto, se resume de la siguiente manera: el 6% realiza ventas por Internet (4% de las micro y 29% de las grandes); el 11% realiza compras a través de este canal; el porcentaje de compras sobre el total de sus adquisiciones que estas empresas realizan en forma electrónica alcanza al 18%. Llama la atención el hecho de que mientras más pequeña es la empresa, mayor es el porcentaje de compras que realiza a través de Internet, lo que se debe fundamentalmente a la menor atomización de sus proveedores e insumos y a la menor complejidad de sus sistemas de adquisiciones. Es decir, una vez que toma la decisión de realizar compras electrónicas, para una empresa más pequeña es más fácil migrar un porcentaje mayor de sus adquisiciones a plataforma Internet.

6.7.- TAMAÑO Y PROYECCIONES DE LA ECONOMÍA DIGITAL EN CHILE

Con el objeto de establecer una medición estructurada del tamaño de la Economía Digital en Chile, el Departamento de Estudios de la CCS construyó indicadores de ventas en cinco grandes subsectores: infraestructura de Tecnologías de la Información y Comunicación; telecomunicaciones; aplicaciones de negocios; servicios (medios de pago, consultoría e investigación, entre otros) y transacciones de comercio electrónico.

Las estimaciones preliminares indican que la Economía Digital habría alcanzado una importancia económica equivalente a US$ 5.532 millones en el año 2000. La mayor parte de este monto corresponde al subsector telecomunicaciones, que aporta unos US$ 3.800 millones a la medición, y que es considerada eje central de la convergencia entre las TI y las comunicaciones, lo que ha permitido potenciar el desarrollo de la economía que gira en torno a Internet.

El subsector de infraestructura, en tanto, habría aportado unos US$ 715 millones en el año 2000, fundamentalmente en hardware y acceso a redes. A continuación se ubica la contribución del comercio electrónico, el que de acuerdo a las estimaciones de la CCS, alcanzó a 465 millones, distribuidos en negocios entre empresas o B2B (91,8%), ventas de empresas a consumidores o B2C (7,7%) y transacciones entre consumidores o C2C (menos del 1%)

Con un tamaño cercano al del comercio electrónico, el subsector servicios de la Economía Digital generó un estimado de US$ 437 millones en 2000, la mayor parte proveniente del segmento consultoría. Finalmente, el subsector de aplicaciones de negocios totalizó US$ 140 millones, principalmente en herramientas de comercio electrónico. Se espera que en los próximos años el sector crezca a tasas promedio del 30%, llegando a superar los US$ 17.000 millones el año 2004. El componente de mayor crecimiento será el comercio electrónico, para el cual se proyecta una acelerado expansión en los próximos cinco años, superando los US$ 10 mil millones el 2004.

CAPITULO III

LA SITUACION INSTITUCIONAL Y POLICIAL EN CHILE

1.- CARABINEROS DE CHILE Y SU INCORPORACIÓN AL PROCESO DE PREVENCIÓN DEL CIBERCRIMEN

1.1.- APRECIACIÓN INTERNA DE CARABINEROS DE CHILE

De la apreciación interna de la problemática Institucional, nos abocaremos al estudio del Informe N°. 26 de fecha 03 de abril del año en curso, de la Dirección de Inteligencia de Carabineros de Chile, de cuyo trabajo podemos extraer:

Ø Aspectos de Seguridad en Redes: La indefensión de las redes computacionales, tanto extra como intra institucional, para la problemática hackers, por lo cual deben disponerse los cursos de acción que permitirán mantener bajo control las amenazas que pudiesen surgir, tanto dentro como fuera del sistema conectado a Internet.

Ø Aspectos de Seguridad de Información: La información de los servicios públicos, privados y las empresas conectadas a Internet, pueden ser vulneradas mediante la aplicación de los llamados virus “caballos de Troya”; permitiendo el acceso indiscriminado a todas sus bases de datos, permitiéndose sustraer, copiar, destruir información desde los discos duros.

Ø Desventajas comparativas con la Policía de Investigaciones:

Determina que el año 2.000, la Policía de Investigaciones de Chile, crea la "Brigada del Cibercrimen, Unidad destinada a la investigación policial de los delitos contemplados en la Ley N°. 19.223. Unidad que ha obtenido asesoría y desarrollo por medio de contactos con el F.B.I. (Federal Bureau of Investigation), permitiéndosele la investigación de diversos hechos de hackers ocurridos en el país.

Determina, erróneamente, la factibilidad y simplificación de las técnicas de investigación utilizadas por el equipo especializado, trabajo de investigación catalogado en todas las áreas del mundo como complicado y de alta complejidad, atendida la volatilidad e fácil eliminación de los elementos de prueba, necesarios para la aplicación de la ley.

Para subsanar dicha apreciación, se adjunta al presente trabajo de Tesis, el anexo N°. 1, denominado "METOLOGIA DE INVESTIGACIÓN CRIMINALISTICA PARA CASOS DE PERPETRACIÓN DE DELITOS INFORMATICOS", acorde a las técnicas de investigación general utilizadas en diversos servicios de investigación criminal informática.

Propuestas de interés sobre las consideraciones:

Ø Señala que la red Institucional, conectada a Internet, de dominio www.carabineros.cl, ip 207.79.140.34, no ha sufrido ningún tipo de ataques durante su permanencia en la red, al contar con medidas de seguridad adecuadas.

Concluye el informe emanado por la Dirección de Inteligencia de Carabineros, en que:

Ø Un estudio superficial sobre la problemática hackers y crakers, y su potencial al ser un nuevo elemento en formación.

Ø Las transgresiones de los hackers, para revelar la información reservada y hacerla pública.

Ø Los acechos de los crakers y su intencionalidad de transgredir normas morales y éticas, basados en la destrucción, daño y venta de información ajena; por beneficios personales y económicos.

Ø La conveniencia Institucional, de preparación tanto profesional como tecnológica para hacer frente a esta problemática mundial y encontrarnos a la par de los requerimientos estatales, judiciales y de la ciudadanía en general, "convirtiéndose en una oportunidad única el poder ser un elemento útil y confiable ante esta nueva forma delictual".

1.2.- APRECIACIÓN EXTERNA DE CARABINEROS DE CHILE

Carabineros de Chile, como una de las Instituciones llamadas por disposición Constitucional a la prevención y control social en la República, ingresa al tercer milenio en una sociedad que evoluciona hacia una realidad cibernética, donde las relaciones personales, comerciales y de gobierno, se desarrollan en un ambiente virtual.

Este ambiente virtual, se ha ampliado sin precedentes gracias a la penetración de la red Internet, dejando de lado fronteras geopolíticas, distancias y por ende legislaciones particulares de cada uno de los países por los cuales desarrollamos nuestras acciones.

Que esta nueva área de acción, ha sido un lugar propicio para el nacimiento de nuevos hechos que ven en el uso de la computadora o como su efecto, actos ilícitos que la comunidad internacional y los distintos países han avizorado como un preocupante acto delincuencial y de graves repercusiones para los distintos actores sociales. 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. Es por ello, que todos los organismos internacionales, han diseñado políticas en los ámbitos legislativos, penal y policial convenientes para enfrentar estos emergentes actos.

Este tipo de hechos, son considerados por los distintos actores como graves, volátiles, transnacionales y socavan la confianza de la gente en las redes como medios de comunicación, incluida la Internet.

Dada la complejidad técnica y jurídica de algunos delitos informáticos, la Comunidad Internacional ha impulsado en los distintos países que componen los distintos foros, la creación de unidades especializadas a escala nacional. Estas unidades especializadas y dependiendo de las características particulares de cada Estado, se encuentra compuestas por personal pluridisciplinar (policial y judicial) y con conocimientos específicos en las áreas de la tecnología, y que cuentan con las instalaciones técnicas adecuadas y funcionales, con los siguientes fines:

· responder rápidamente a las solicitudes de información sobre presuntos delitos.

· Actuar como interfaz de las autoridades competentes, nacional e internacionalmente.

· Mejorar o desarrollar técnicas especializadas de investigación informática con el fin de detectar, investigar y procesar delitos informáticos;

· Actuar como centro de excelencia en cuestiones relacionadas con la delincuencia cibernética, con el fin de compartir experiencias y mejores prácticas.

En la UE., EE.UU., y otras regiones del mundo, se han creado las unidades especializadas que tratan los delitos informáticos.

A nivel sudamericano, las experiencias de la Policía Nacional de Argentina y de la Policía de Investigaciones de Chile, apuntan al resguardo y control de los distintos tópicos que determinan sus legislaciones sobre los delitos informáticos; siendo estos pioneros en Sudamérica en estas nuevas áreas delincuencial y de aplicación de la Ley.

En tanto, pese al sostenido crecimiento de estos servicios policiales altamente tecnificados y especializados en el control formal de los delitos informáticos; más aun cuando nuestra economía se encamina hacia una globalización y aumento en la participación de la economía digital y el Gobierno de Chile, fomenta el uso intensivo de estas nuevas tecnologías para lograr el acercamiento y entrega de mejores servicios para la comunidad, dando los primeros pasos hacia el establecimiento del Gobierno Digital, Carabineros de Chile pese a estos alentadores escenarios para un desarrollo en este nuevo paradigma no ha desarrollado ninguna acción para alcanzar el acelerado desarrollo, en esta área, de la tecnología digital; más aún cuando nuestro referente como es la Policía de Investigaciones de Chile, se posiciona con el transcurrir del tiempo en esta área, haciéndose participe en las actividades sectoriales del gobierno para el desarrollo programático de las tecnologías digitales en Chile.

Los niveles de crecimiento esperado para Internet en Chile, en la actualidad el número de usuarios conectados a Internet, supera 1.824.000 y con una estimación para el año 2005 que supera a los 4.500.000 usuarios, lo que representa a la población nacional entre un 12% y 28% aproximadamente.

En el ámbito comercial, las proyecciones estimadas por la Cámara de Comercio de Santiago, ubica a toda la economía digital en torno a los MUS$ 7.400 en el año 2001 y con una tasa de crecimiento real de un 30% anual, se estima que el año 2005, estos valores alcanzarán cerca de los MUS$ 12.000.

2.- RESPONSABILIDADES ENTREGADAS A LOS ORGANISMOS POLICIALES CHILENOS

2.1.- POLICIA DE INVESTIGACIONES DE CHILE

Policía de Investigaciones de Chile, crea en el transcurso de agosto del año 2000 la Brigada de

Investigación de Delitos Informáticos o Cibercrimen, dedicado exclusivamente al rastreo, prevención y control de los delitos de carácter informático que ocurren dentro de la República de Chile. Principalmente con ocasión de los diversos hechos relacionados con “hackers” a sitios oficiales del gobierno y defraudaciones a empresas privadas. Se caracteriza por ser única en su especie dentro de América Latina. Se relaciona directamente con el FBI, donde recibe capacitación e intercambio de materias de estudios de los delitos informáticos.

Sus misiones institucionales son:

- Aportar los medios probatorios al tribunal, cuando se detecta la utilización de herramientas y/o tecnologías de la información, en la comisión de delitos.

- Detectar e investigar conductas ilícitas en Internet, referidas principalmente al comercio electrónico y hacking de sitios y servidores Web.

- Capacitar y formar investigadores especialistas en delitos informáticos.

Como función inmediata, esta brigada ha asesorado a las unidades operativas en la investigación referida a la criminalidad informática, específicamente sobre conductas ilícitas cometidas en Internet, además forma parte del grupo de trabajo chile@futuro, correspondiente a una alianza público privada para el desarrollo de Internet en el país y otras comisiones cuyo propósito es sentar las bases estructurales en cuanto al uso de las tecnologías de información, la identificación de delitos informáticos conductas ilícitas y la formación de alianzas estratégicas para el combate y prevención de estas conductas.

2.2.- INSTITUCIONES PRIVADAS

En el ámbito nacional, no existen empresas de servicios privados que vendan o entreguen este tipo de servicio de investigación en el ámbito de los delitos informáticos-forense, se circunscriben generalmente a la venta de Seguridad Informática en hardware y software.

CAPITULO IV

1.- CONCLUSIONES

A través del desarrollo del trabajo de la presente tesis, sobre los delitos informáticos, delitos considerados emergentes para el milenio que comienza y por ser de un carácter exploratorio y en base a todos los antecedentes recopilados, bibliografía recopilada y entrevistas realizadas, el alumno tesista logra llegar a las siguientes conclusiones sobre el tema tratado:

Ø Que desde el inicio del proyecto Arpa en el año 1967, el desarrollo de Internet en estos 33 años, ha permitido el surgimiento de una nueva era en las comunicaciones e interrelaciones humanas, comerciales y de gestión.

Ø Que este nuevo paradigma en las relaciones humanas, permite acercar distancias, eliminar barreras y deponer conflictos raciales, religiosos, culturales.

Ø Que si bien existe una nueva forma de comunicación social y humana, esto ha dado margen al surgimiento de nuevos hechos o delitos, que valiéndose de la red, de sus computadores como medio o como fin, logran transgredir y superar ampliamente las distintas figuras típicas penales.

Ø Que las técnicas informáticas han creado nuevas posibilidades del uso indebido de las computadoras, lo que ha generado la necesidad de una regulación por parte del derecho.

Ø Se ha generalizado el entendimiento de que “Delitos Informáticos”, son todas aquellas conductas ilícitas susceptibles de ser sancionados por el derecho penal, que hacen uso indebido de cualquier medio informático.

Ø La Criminología, se ha abocado al estudio de los delitos informáticos, desde el punto de vista del delincuente, del delito, la norma y el control social.

Ø Del delincuente, ha determinado que los delincuentes informáticos, son de conductas llamados “delitos de cuello blanco”, ya que no es de acuerdo al interés protegido, sino de acuerdo al sujeto activo que los comete, catalogando al delincuente como persona de cierto status económico, la comisión del delito, no encuentra explicación en la pobreza, ni mala habitación, ni por carencia de recreación, etc.

Ø Se ha determinado, que el autor de este tipo de delitos no es fácil descubrirlo ni sancionarlo, existe una indiferencia en la opinión pública sobre los daños ocasionados en la sociedad, ya que esta no los considera delincuentes, no los segrega, no los desprecia ni los desvaloriza, por el contrario, el autor se considera respetable y generalmente son sancionados con medidas de carácter administrativo y no privativos de la libertad

Ø Los problemas jurídicos relacionados con la Internet, se basan especialmente en los nombres de dominio y las marcas comerciales, al existir diferencias en su posesión y administración por parte de sus propietarios; de los derechos de autor, ante la imposibilidad de prohibir las reproducciones no autorizadas de trabajos y elementos de propiedad intelectual, la realización virtual de actividades altamente reguladas en los ámbitos financieros, de compra y venta de valores; al no existir fronteras ni el control adecuado sobre las incipientes instituciones mercantiles, que hacen uso de la red como sustento

de su trabajo.

Ø El comercio electrónico desarrollo gracias a la proliferación de la Internet, los problemas más urgentes se basan en la formación del consentimiento, la seguridad acerca de las identidades de los contratantes y la prueba de las obligaciones; como también es sobre la legislación aplicable al acto o contrato específico, los tribunales competentes y la seguridad en los medios de pago; para ello las distintas legislaciones a nivel mundial y gracias a la promulgación de la Ley Modelo sobre el Comercio electrónico, de la Comisiòn de las Naciones Unidad para el Derecho Comercial (UNCITRAL), que recomienda a los países integrantes de las Naciones Unidas, sobre la legislación nacional en materia de las firmas y documentos electrónicos, con el objeto de dar seguridad a las relaciones jurídicas electrónicas.

Ø Chile, en parte adopta dicho criterio, mediante el establecimiento del Decreto Supremo N°. 81, de 1999, del Ministerio Secretaría General de la Presidencia, que regula el uso de la firma digital y los documentos electrónicos en la Administración del Estado, otorgando a la firma digital los mismos efectos que la firma manuscrita, eliminando de esta forma la necesidad de sellos, timbres y vistos buenos.

Ø Que el Congreso Nacional, actualmente tiene a trámite legislativo el Proyecto de Ley N°. 158-342, de fecha 09 de agosto de 2000 mantiene el estudio sobre las Comunicaciones Electrónicas, que trata acerca de las transmisiones electrónicas y la prestación de servicios de certificación y otras; todas recomendaciones de UNCITRAL.

Ø En el Derecho Penal informático, Chile se destaca al ser el primero en promulgar una ley que tipifica figuras relativas a la informática, promulgada la Ley N°. 19.223, de fecha 28-05-1993, tengo que entró en vigencia el 07 de Junio de 1993; en esta ley la destrucción, inutilización, sustracción, modificación en los sistemas de información, de los datos contenidos dentro de una computadora es castigada con penas que van desde un año y medio a cinco años de prisión.

Ø Que nuestra legislación de Procedimiento Penal o Procesal Penal, según corresponda, se ha adelantado al considerar en las modificaciones del Art. 113 bis, del año 1989, al admitir como elementos de prueba, “cualquier medio apto para producir fe”, y la autorización al Juez, para el esclarecimiento de los hechos de “valerse de resultados obtenidos por la utilización de aparatos destinados a desarrollar exámenes o demostraciones científicas o por medio de la computación”; dando a estos elementos otorgados por la computación, es decir no les otorga un carácter de instrumento, sino los considera un documento y los estima como base de presunciones o indicios. Que dicho criterio se ha mantenido para la redacción y aplicación del Código de Procesal Penal, en el capítulo IX, de la Prueba, Párrafo 1º, Art. 202º y ss.

Ø La legislación penal comparada con otros países occidentales, ha demostrado la importancia que ha revestido en estos últimos años la aplicación e incorporación en la legislación penal de los delitos informáticos, es así como Alemania, Austria, Francia, Estados Unidos de Norteamérica, España y Perú, dando mayor o menor énfasis en el control formal de estos delitos emergentes.

Ø En la mayoría de los casos, los daños mediante la destrucción o alteración de datos, programas o documentos electrónicos, estafas, amenazas, calumnias o injurias, pornografía infantil, cometidos por medio de sistemas computacionales son sometidos como delitos informáticos.

Ø La comunidad internacional, se ha abocado al control de los delitos informáticos, destacándose la labor desarrollada por la Organización de las Naciones Unidas; que ha dado el reconocimiento de delito a distintas acciones ocasionadas por medio o como fin de la computadora, entre los que destacamos; los fraudes cometidos mediante manipulación de computadoras, manipulación de programas, manipulación de los datos de salida.

Ø También elaboró el " Manual sobre la prevención y el control de la delincuencia informática", que se ha actualizado recientemente, que se basa en un estudio sobre la posibilidad de aplicar a escala internacional y armonizar los derechos penales para abordar el problema del abuso informático o de la delincuencia informática, como también en el año 1986, publica el informe "Delincuencia Informática: Análisis de las medidas jurídicas", donde se examinan las leyes y propuestas existentes para la reforma en los Estados miembros y se recomienda una lista mínima de abusos que los países debería controlar y penalizar con leyes penales ordinarias.

Ø La Unión Europea, que ha desarrollado amplios cursos de acción para la prevención y control de los delitos informáticos, con una importante actividad en el ámbito político, judicial, policial. A fin de lograr que el éxito de la sociedad de la información es importante para el crecimiento, la competitividad y las posibilidades de empleo en Europa; como también las repercusiones económicas, sociales y jurídicas.

Ø La UE, para la lucha contra los contenidos ilícitos y nocivos en Internet, para la protección de la propiedad intelectual y los datos personales, para la promoción del comercio electrónico y el uso de la firma electrónica, presento al Consejo de Países Miembros el estudio sobre la Delincuencia Informática, de nombre COMCRIME, para su estudio y realización de tareas concretas en esta área y estrategias contra la delincuencia de alta tecnología.

Ø La UE., ha promovido la creación, donde no exista, de Unidades Policiales especializadas en delincuencia informática a escala nacional, apoyar la formación técnica pertinente para la aplicación de la ley y fomentar las acciones europeas tendientes a la seguridad de la información.

Ø En el plano técnico y en línea con el marco jurídico, la Comisión promoverá el desarrollo Informático, para comprender y reducir los puntos vulnerables, estimulará la difusión de conocimientos técnicos.

Ø Se ha determinado que la complejidad técnica y jurídica de algunos delitos informáticos, la Comunidad Europea ha dado importancia a la creación de unidades especializadas a escala nacional, compuestas por personal pluridisciplinar (policial y judicial), con conocimientos especializados, instalaciones técnicas adecuadas; con objetivos de mejorar o desarrollar técnicas especializadas de investigación informática, con el fin de detectar, investigar y procesar delitos informáticos.

Ø Diversos países han creado y apoyado la formación de Unidades Policiales especializadas, dentro de las que destacamos: ITC: Information Techology Crime de INTERPOL, Internet Fraud Complation Center (FBI/NW3C) del FBI, Unidad de Investigación de Delincuencia en Tecnologías de la Información del Cuerpo Nacional de la Policía Española; Oficina Central de Lucha contra la Criminalidad Ligada a las Tecnologías de la Información y las Comunicaciones de la Policía Nacional de la República de

Francia.

Ø Desde el punto de vista económico, la economía digital ha permitido una revolución en la actividad económica mundial, con alcances sin precedentes, ya que las Tecnologías de la Información apuntan hacia la optimización del uso de los recursos en las empresas.

Ø En Chile, los efectos de la demanda de TI. ha generado gastos sobre los MUS$ 1.138, reflejando un crecimiento anual promedio de 16%, pasando desde el año 1985 de un 0,8% del PIB a 1,7%.

Ø Las más recientes inversiones en el área de la seguridad informática, van en directa relación con la implementación de tecnologías que otorgan seguridad al comercio electrónico, en gran medida por el traspaso de las grandes empresas al comercio electrónico en Internet.

Ø La rápida penetración de Internet en Chile, ha dado paso a una necesidad de la certificación para el uso seguro de las transacciones comerciales, naciendo en Chile las empresas Certificadoras, que como principal objetivo es la autentificación, confidencialidad, integridad y no repudio; que son los fundamentos de la certificación digital.

Ø Se estima que en el año 2000, la cantidad de internautas en Chile alcanzó al 9% de la población y se espera que para el año 2005, ascienda al 25 % de la población

Ø En cuanto a los valores de las transacciones a través de la red Internet en Chile, alcanzó en Chile aproximadamente a MUS$ 5.532 y se proyecta para el año 2005 un nivel de transacciones de aproximadamente MUS$ 12.000

Ø En esta visión de la realidad en Chile y la penetración de la Internet, nuestro país ha creado la Brigada de Delitos Cibercrimen, unidad destinada a la investigación policial de los delitos contemplados en la Ley N°. 19.223

Ø Tiene como finalidad la de aportar los medios probatorios al tribunal, detectar e investigar conductas ilícitas en Internet, capacitar y formar investigadores especialistas en delitos informáticos.

Ø Participa activamente en el grupo de trabajo chile@futuro, que propende al desarrollo informático en Chile

Ø Carabineros de Chile, no posee sección, departamento ni Unidad dedicada al estudio y persecución de los delitos informáticos.

Ø La Dirección de Inteligencia de Carabineros, mediante su Informe N°. 26, de fecha 03 de abril del año en curso, determina la creciente realidad de la problemática hackers en el país.

Ø Estima la conveniencia Institucional, de la preparación tanto profesional como tecnológica para hacer frente a la problemática mundial y encontrarnos a la par de los requerimientos estatales, judiciales y de la ciudadanía en general, “convirtiéndose en una oportunidad única, el poder ser un elemento útil y confiable ante esta nueva forma delictual”

Ø Que en base a esta nueva problemática, se ha logrado la confección de una Metodología Forense Informática, que permite el trabajo en el Sitio Informático de Hackeo.

Ø No existe en el mercado nacional, empresa o servicio dedicado a la investigación forense de la problemática informática, que sirva de apoyo a la labor de los Fiscales o los Tribunales de Justicia.

2.- PROPUESTAS

En base a las conclusiones arribadas en este trabajo de Tesis, se propone a esta Honorable Comisión, las siguientes propuestas y cursos de acción para el accionar de Carabineros de Chile y esta Academia de Ciencias Policiales, las que paso a detallar:

2.1.-ÁMBITO DE CARABINEROS DE CHILE:

Ø Participación en todas las entidades Nacionales e Internacionales, importen estudios sobre las bases de la Tecnología Informática en Chile.

Ø Acercamiento y realizar Convenios Internacionales, con Organismos supranacionales que tengan injerencia en la problemática de la Delincuencia Informática.

Ø Creación en Carabineros de Chile, de una sección, unidad o departamento; que permita el estudio avanzado de los delitos informáticos y sus consecuencias; que sirva de apoyo a la labor de los Tribunales de Justicia en la investigación de los delitos y como ente preventivo de delitos cometidos por medio de la red Internet, para lo cual se adjunta anexo del proyecto de formación.

Ø Capacitación en todos los organismos internacionales y policiales extranjeros, que acorde a la Organización de las Naciones Unidas deben proceder a la cooperación internacional para el control de los Delitos Informáticos.

Ø Participar en instancias legislativas, que permitan mejorar la calidad de nuestra ley sobre delitos informáticos.

2.2.- ÁMBITO ACADÉMICO:

Ø Incorporación en las mallas curriculares en todos los planteles de estudios institucionales, y en la Academia de Ciencias Policiales en su Curso de Alto Mando y Carreras de Ingeniería, el estudio de la problemática emergente del siglo XXI, en el campo de los delitos informáticos.

Ø Conformación en los planteles de estudios institucionales, de cursos de capacitación y formación

profesional sobre la implementación de la Metodología de Informática Forense.

Ø Participación de la Academia de Ciencias Policiales de Carabineros, en los foros que se realicen con motivo de esta problemática delictual emergente.

BIBLIOGRAFIA

1.- INGENIERIA EN REDES, López José, Curso Ingeniería Informática.

2.- INFORMATIVO ACADEMICO, Lázzaro Luis, Santiago de Chile, Chile, 1996.

3.- COMPUTER CRIME, Bureau of Justice Statistics, 1ra. Edición, US. Department, EE:UU. 1981

4.- REDES DE AREA LOCAL, Alfredo Abad - Mariano Madrid, 1era. Edición, 1998, Mc Graw-Hill/interamericana de España, Madrid, España.

5.- LEYES Y NEGOCIOS, Oliver Hance, 1era. Edición en español, 1996, Programas Educativos S.A., D.F. México, México.

6.- SECRETS OF A HACKER, Dennis Fiery, 1ra. Edición, 1994, Loompanics Unlimited, San Francisco, EE.UU.

7.- HACKING EXPOSED, STUART MCCLURE y OTROS, 1ra. Edición, 1999, McGraw-Hill, Berkeley, california, EE.UU.

8.- Creación de una Sociedad de la información más segura, Comisión de la Comunidad Europea, 1ra. Edición, 2001, Bruselas, Comunidad Europea.

9.-Chile en la era digital, una urgencia nacional, Fernando Prieto Domínguez, 1ra. Edición, mayo 2000, Acti, Santiago de Chile, Chile.

10.- Empresas Chilenas en Internet, UCA-FACEA-Univ. De Chile, 1ra. Edición, 2001, Santiago de Chile, Chile.

11.- Economía Digital en Chile, Cámara de Comercio de Santiago, 1ra. Edición, 2001, Santiago de Chile, Chile.

12.- Mensaje Presidencial N°. 158-342, Presidencia de la República, sin edición, 2000, Santiago de Chile, Chile.

13.- Ley N°. 19.223 Sobre Delitos informáticos, República de Chile, sin edición, 1993, Santiago de Chile, Chile.

14.- Código de Procedimiento Penal, República de Chile, 2000, Santiago de Chile, Chile

15.- Código de Procesal Penal, República de Chile, 1ra. Edición, 2000, Santiago de Chile, Chile.

6.1.2.- TRANSACCIONES EN LA ECONOMIA DIGITAL 63

PETRACION DE DELITOS INFORMATICOS.

N°2 PROYECTO FORMACION Y ESTRUCTURA SECCION PREVENCION Y CONTROL DELITOS INFORMATICOS