

# **Nuevos desafíos del derecho en la economía digital**

Autor:

Doctor Diego Marcelo Sánchez Montenegro  
Quito-Ecuador

Año 2.002

## **DEDICATORIA**

A mi abuelo Doctor Pedro Nel Montenegro Cabrera, hombre de principios e ideales.

# Contenido

<b>CONTENIDO</b>	<b>3</b>
<b>SÍNTESIS</b>	<b>5</b>
<b>INTRODUCCIÓN</b>	<b>5</b>
<b>CAPITULO I: GENERALIDADES DE LOS DELITOS INFORMÁTICOS.</b>	<b>7</b>
1.- ANTECEDENTES.	7
1.1.- LA GLOBALIZACIÓN Y LA INFORMÁTICA	7
1.2.- EL CIBER ESPACIO: INTERNET.	8
1.3.- EL DERECHO INFORMÁTICO.-	10
2.- CONCEPTO DE DELITO INFORMÁTICO.-	13
<b>CAPITULO II: MARCO JURÍDICO Y CARACTERES DE LOS DELITOS INFORMÁTICOS</b>	<b>16</b>
1. - PRINCIPIO DE LEGALIDAD Y RESERVA.-	16
2. BIENES JURÍDICOS A SER PROTEGIDOS.	18
2.1.- DERECHO A LA INTIMIDAD.	18
2.2. - DERECHO A LA INFORMACIÓN.	24
2.3. - DERECHOS PATRIMONIALES.	24
2.4. - SEGURIDAD NACIONAL.	25
3. SUJETO ACTIVO DEL DELITO INFORMÁTICO.	25
4. SUJETO PASIVO DEL DELITO INFORMÁTICO.	26
<b>CAPITULO III: CLASIFICACION DE LOS DELITOS INFORMÁTICOS:</b>	<b>27</b>
1.- DELITOS INFORMÁTICOS COMETIDOS COMO FIN U OBJETIVO.	27
1.1- ACCESO Y DIVULGACIÓN NO AUTORIZADOS A SERVICIOS Y SISTEMAS INFORMÁTICOS.	27
1.2.- DAÑOS O MODIFICACIONES DE PROGRAMAS O DATOS COMPUTALIZADOS.	30
1.3.- FRAUDE INFORMÁTICO.-	33
1.4.- TRANSFERENCIA DE FONDOS.	35
1.5.- SABOTAJE INFORMÁTICO	35
CLASES O TIPOS DE SABOTAJE INFORMÁTICO:	36
2.- DELITOS INFORMÁTICOS COMETIDOS COMO MEDIO O INSTRUMENTO PARA PERPETRAR OTROS DELITOS.	38
2.1.- PORNOGRAFÍA.	38
2.2.- NARCOTRÁFICO.	39
2.3.- TERRORISMO.	40
2.4.- ESPIONAJE.	40
2.5.- ESPIONAJE INDUSTRIAL.	41
<b>CAPITULO IV: LOS DELITOS INFORMÁTICOS EN EL DERECHO COMPARADO</b>	<b>42</b>
1.GENERALIDADES	42
2. LEGISLACIONES COMPARADAS	42
2.1. - LEGISLACIÓN DE LOS ESTADOS UNIDOS DE AMÉRICA	42
2.2. - LEGISLACIÓN DE LA COMUNIDAD ECONÓMICA EUROPEA.	43
2.3. - LEGISLACIÓN DE LA REPÚBLICA DE CHILE.	51
2.4. - LEGISLACIÓN DE LOS ESTADOS UNIDOS MEXICANOS.	51
2.5. - LEGISLACIÓN DE LA REPÚBLICA DE COLOMBIA.	52

2.6. - LEGISLACIÓN DE LA REPÚBLICA DEL PERÚ.	54
3. - ORGANISMOS INTERNACIONALES DE PREVENCIÓN DE DELITOS INFORMÁTICOS.	55

**CAPITULO V: PROPUESTA DE TIPIFICACIÓN DE DELITOS INFORMÁTICOS EN LA LEGISLACIÓN PENAL ECUATORIANA:** **57**

1.- IDEAS GENERALES	57
2.- DELITOS CONTEMPLADOS EN LA LEY DE PROPIEDAD INTELECTUAL DE LA REPÚBLICA DEL ECUADOR.	58
3.- PROYECTO DE LEY QUE CONTEMPLA LOS DELITOS INFORMÁTICOS	60
2.- SEGUNDA SENTENCIA RELATIVA A DELITOS INFORMÁTICOS. CASO HISPAAHACK. BARCELONA - ESPAÑA.-	70

**GLOSARIO DE TÉRMINOS** **74**

**CONCLUSIONES** **78**

**RECOMENDACIONES** **78**

**1.-BIBLIOGRAFÍA PRINCIPAL.-** **79**

**2.-BIBLIOGRAFIA COMPLEMENTARIA** **81**

# Síntesis

SÍNTESIS DE LA OBRA LOS DELITOS INFORMÁTICOS: CONDUCTAS DELICTIVAS QUE DEBEN TIPIFICARSE EN LA LEGISLACIÓN PENAL ECUATORIANA.

**Capítulo I.-** La investigación se inicia con una aproximación hacia los conceptos de globalización, Informática, Nuevas Tecnologías y la relación con las Ciencias Jurídicas. Se analizan los conceptos del Derecho Informático así como sus particularidades específicas. Se formula y estudia los diversos conceptos de delito informático.

**Capítulo II.-** En esta parte del trabajo se investigan los bienes jurídicos que se lesionan por el cometimiento de los delitos informáticos. Se realiza un análisis de las normas consagradas en la Constitución Política de la República del Ecuador y se estudia al sujeto activo y pasivo del delito informático.

**Capítulo III.-** La clasificación de los delitos informáticos forma parte sustancial del Capítulo III. En él se analizan algunas de las conductas que se tipifican en otros países como delitos informáticos. Se estudia los delitos informáticos cometidos como fin u objetivo y aquellos delitos que son medios para perpetrar otros delitos.

**Capítulo IV.-** Con la finalidad de conocer y estudiar como varios países del mundo han legislado la materia correspondiente a delitos informáticos se incorporan en este capítulo varias normas legales que regulan y sancionan este tipo de ilícitos.

**Capítulo V.-** Se realiza un estudio acerca de los delitos que se encuentran insertos en la Ley de Propiedad Intelectual de la República del Ecuador. Se establece un proyecto de ley que regula y tipifica los delitos penales y que sugerimos se incluyan en el Código Penal Ecuatoriano.

## INTRODUCCIÓN

El desarrollo de los sistemas informáticos en la actualidad y sobre todo el apareamiento de la red mundial de información que se ha denominado Internet, han generado el apareamiento de conductas delictivas que no se encuentran tipificadas en el Código penal ecuatoriano.

La falta de tipificación tiene como consecuencia que las personas que cometen esos ilícitos, los delincuentes informáticos, queden en total impunidad. De tal forma que los perjuicios que se ocasionan a las personas naturales, y a las personas jurídicas de derecho público y privado no se sancionen en la República del Ecuador, debido a que no existe una normativa al respecto.

El propósito de la investigación es el proveer a los lectores y a la comunidad en general, de conocimientos básicos e imprescindible sobre los delitos informáticos y establecer una propuesta de normas penales que castiguen esa serie de ilícitos cometidos por los delincuentes informáticos.

El desconocimiento del tema por parte de los legisladores, magistrados, jueces, abogados, asesores legales y de la sociedad ecuatoriana en general, y la importancia de establecer una normativa penal que precautele los intereses de la sociedad, constituyen el principal interés de haber elegido este tema de investigación.

Los métodos que se aplicarán a este trabajo son los siguientes:

1.- Método Analítico-Sintético.- Ya que es necesario determinar, mediante un razonamiento analítico-sintético, cuales son las circunstancias que determinaron que los legisladores, magistrados, jueces, abogados, asesores legales y la sociedad en general, no hayan tomado en cuenta las conductas delictivas que provienen del uso del ordenador y del internet.

2.- Método Dialéctico.- La aplicación de este método servirá de base para hacer comprender a los legisladores, magistrados, jueces, abogados, asesores legales y a la sociedad en general, que el tema está sujeto a varias reformas legales. Este método será muy necesario para comprender que los criterios de los tratadistas jurídicos también están sujetos a cambios.

3.- Método Histórico Comparado.- Se justifica su aplicación en nuestra investigación, ya que haremos referencias a los antecedentes históricos de los delitos informáticos. De forma tal que haremos aportes y sugerencias constructivas que son de vital importancia en el presente trabajo de investigación.

# **CAPITULO I: GENERALIDADES DE LOS DELITOS INFORMÁTICOS.**

## **1.- Antecedentes.**

### ***1.1.- La globalización y la informática***

La globalización se evidencia en todos los órdenes de la realidad de la sociedad de fines del siglo XX y principios del siglo XXI, y se manifiesta en una sumatoria de cambios tecnológicos, económicos, sociales, culturales y por ende cambios en la ciencia jurídica.

Como antecedente de la globalización mencionaremos los esfuerzos de algunos países vencedores de la contienda que se denominó la Segunda Guerra Mundial, en establecer un nuevo orden internacional que se plasmaría en la creación de las Naciones Unidas, y en una serie de organismos adscritos a la O.N.U., que velarían por la paz mundial y desarrollo el crecimiento económico de todos los países.<sup>1</sup>

La globalización para el Dr. Horacio Godoy es “... un proceso complejo, de carácter multisectorial, que se desarrolla en forma vertiginosa las relaciones intersectoriales en escala mundial. Y que genera un nuevo escenario de alcance mundial, con procesos globales, actores globales, problemas globales, posibilidades y riesgos globales. Ha cambiado la escala de fenómenos a estudiar, ha cambiado el ritmo de los acontecimientos y han cambiado el contenido de los conocimientos que se expresan en las más diversas actitudes.”<sup>2</sup>

Esta nueva forma de desarrollo de la humanidad, la globalización, tiene como uno de los pilares fundamentales el desarrollo de la informática. De esta forma pensamos que los procesos de globalización van de la mano con el desarrollo vertiginoso de los sistemas informáticos. La tecnología actual permite por ejemplo a una persona enterarse de mercados bursátiles tan distantes como el de la bolsa de valores de Nueva York, Tokio, Londres, Barcelona, e iniciar transacciones financieras con una ejecución y eficiencia inmediatas.

La era de la informática ha sido calificada por Alvin Toffler como la “Tercera Ola.”<sup>3</sup> Siguiendo a este autor, plantea que la primera gran ola se presentó en la historia de la humanidad cuando los humanos descubrieron la agricultura y por lo tanto comenzaron a diversificar su trabajo y sus medios de producción. La segunda ola se inició con la revolución industrial y se desarrolló en el continente europeo a finales del siglo XVII. Estos sucesos mundiales trajeron como consecuencia un cambio radical en las relaciones entre los seres humanos, como radical y vertiginoso es el cambio que experimenta la humanidad a finales del Siglo XX y principios del Siglo XXI, con el desarrollo de la informática.

La revolución informática se desarrolla a finales de la década de 1970, y abarca campos tan disímiles como las comunicaciones, el transporte, la inteligencia artificial, las ciencias exactas, la exploración del espacio, entre otras; y hace que el ordenador sea un instrumento imprescindible para el desarrollo de las actividades normales y cotidianas de personas naturales y jurídicas en el globo terrestre.

<sup>1</sup> Carta de las Naciones Unidas. Ed. Porrúa. 1995.

<sup>2</sup> GODOY Horacio, “Reflexiones sobre el proceso de globalización”, Centro Latinoamericano de Globalización y Prospectiva, 1994.

<sup>3</sup> TOFFLER Alvin, “La creación de una nueva civilización”, Ed. Plaza & Janes Editores S.A., Barcelona, 1996.

## **1.2.- El ciber espacio: Internet.**

---

El desarrollo del Internet se debió en gran parte a un proyecto de estrategia de inteligencia militar desarrollada por los Estados Unidos de América.

A principios de la década de 1960, el Departamento de Defensa (DoD por sus siglas en inglés) de los Estados Unidos de América (E.U.A) por sus siglas en español, estudia la creación de una red de comunicaciones entre ordenadores con el objetivo de compartir información de manera inmediata, fidedigna y segura.

La idea fundamental se basó en que algunos de los ordenadores de las agencias de inteligencia de los E.U.A., se encuentren conectados en red mediante conexiones telefónicas, así estarían en igual capacidad de transmitir, enviar y recibir mensajes a cualquier parte del mundo en donde se encuentre una línea telefónica. El mensaje enviado es dividido en paquetes, cada uno con la información suficiente para llegar a su destino, por lo que el viaje a través de la red sería independiente. La ruta que cada paquete sigue no tendría importancia, lo importante es que el mensaje llegue a su destinatario final.

La primera red de investigación científica fue realizada por la Advanced Research Projects Agency (ARPA). En el mes de diciembre de 1969 se conectaron cuatro ordenadores, tres en el estado de California - E.U.A. y una en el estado de Utah - E.U.A., en la red que se conoció como ARPANET. Gracias a esta red, científicos e investigadores podían intercambiar información y hacer uso de facilidades de forma remota. La estructura descentralizada de la red hacía fácil su expansión. El tipo de computadora que se conectara no era importante; sólo debía ser capaz de poder "hablar el mismo lenguaje" basado en el principio de enviar la información fragmentada en paquetes.

Originalmente el lenguaje informático utilizado por ARPANET fue NCP (Network Control Protocol). Luego fue sustituido por uno más sofisticado conocido como TCP/IP. TCP (Transmission Control Protocol) Protocolo de Control de Transmisión, que es el programa responsable de convertir el mensaje en paquetes y luego reconstruirlo en el destino. IP (Internet Protocol) Protocolo de Internet, es el que direcciona el envío de los paquetes a través de distintos nodos y redes dada la dirección de su destino. El software que implementaba los protocolos de TCP/IP en las computadoras era de fácil acceso, gratis y dado el carácter descentralizado de la red, permitieron que cada día se enlazaran más ordenadores.

En la década de 1980 se desarrollan un conglomerado de redes, como por ejemplo: BITNET, CSNET, NSFNET, así como redes de las agencias gubernamentales de los E.U.A., tales como la NASA, el Instituto Nacional de Salud y el Departamento de Energía.

Con la finalidad de organizar un sistemas de dominios para distinguir a que grupo o ubicación geográfica pertenece cada servidor, éstos fueron nominados por su localización geográfica en idioma inglés (us, fr, ec, co, etc.) El resto de nodos fueron agrupados en seis distintos dominios, de igual forma en idioma inglés (edu, .gov, .mil, .com, .org y .net). Los dominios .edu, .gov y .mil pertenecen a instituciones educativas, gubernamentales y militares respectivamente. Estos dominios fueron los pioneros en ARPANET, por otra parte el dominio (.com), pertenece a instituciones comerciales, (.org) a organizaciones sin fines de lucro y (.net) a redes que sirven de enlace o apoyo a otras redes.

En la reunión del Grupo de los ocho (G8), que conforman los siete países más industrializados del planeta y Rusia, decidieron en la reunión realizada en Yokohama - Japón en Julio del 2.000, aumentar siete denominaciones más, entre las que se señalan (.biz) (.name) (.shop) (.travel) (.bank)<sup>4</sup>.

En 1992 se crea el Internet Society (Sociedad Internet) con el propósito de estandarizar protocolos en el Internet y proveer organización a tan creciente movimiento. Para ese momento el número de computadoras conectadas superaba el millón.

---

<sup>4</sup> IRIARTE Erik, Primer Encuentro de Derecho e Informática, Quito, julio del 2.000.

El año 1994 fue muy importante en la historia del Internet. En este año se eliminan las restricciones para que empresas comerciales utilicen el Internet. A partir de entonces el interés de parte del sector privado y comercial hace que el Internet llame la atención de los medios.

Para fines de 1994 había más de 3.8 millones de servidores registrados y más de 30 millones de usuarios. Las oportunidades comerciales, educativas y de acceso a la información para todo tipo de aplicación se multiplicaron a partir de esa fecha.

Las últimas estadísticas demuestran que el crecimiento exponencial continúa y se estima en más de 200 millones de usuarios que tienen acceso al Internet.<sup>5</sup>

Programas de uso remoto de computadoras, transferencias de archivos entre computadoras y correo electrónico fueron y continúan siendo los puntos básicos del Internet. Luego surgen las listas automáticas de correo electrónico y los distribuidores de servidores, mediante estos últimos dos servicios es posible compartir ideas e información con grupos de interés común, en forma de grupos de discusión en donde lo que aporta un usuario es distribuido a los demás suscriptores del grupo<sup>6</sup>. Hoy es posible encontrar grupos de discusión que abarcan una inmensa variedad de temas. Además a través de estos servicios se distribuyen numerosas publicaciones y resúmenes semanales o diarios.<sup>7</sup>

Sin embargo son los servicios interactivos de información los que más interesan a la comunidad del Internet; servicios donde los usuarios pueden visualizar y copiar información específica al instante. Servicios como el World Wide Web, www por sus siglas en inglés, permiten este tipo de interacción.

Para obtener acceso a los servicios de la Red Mundial (www) es necesario contar con un programa que se conoce como navegador, llámese este Netscape, Explorer u otros. Este programa permite la accesibilidad a computadoras en el Internet que permite la visualización de información de una forma rápida y fácil haciendo uso de recursos de multimedia (sonidos, gráficos, videos, animaciones, etc.). De allí que un alto porcentaje del tráfico mundial de información se produce en este tipo de red en el Internet.

La búsqueda de datos e información en Internet se puede efectuar a través de motores de búsqueda que relacionan los temas de información con las direcciones electrónicas y con los textos que en ellas constan. Servicios como Google, Alta Vista, Excite, Infoseek, Webcrawler, Go, Bacán, entre otros, permiten hacer búsquedas por frases o palabras claves. De esta forma podemos llegar a dar con la información que deseamos más fácilmente.

La explosiva expansión del Internet, se hace evidente ya que en julio del 2000, se incrementan al día más de dos millones de páginas de información, en una red mundial que se calculaba, a principios del año 2000, en cinco millones de sitios que contienen más de mil quinientos millones de páginas de información y datos.<sup>8</sup>

La abolición de las restricciones que existían para el sector comercial marcó un punto importante en la historia del Internet. Esto se ha demostrado con el exponencial crecimiento que experimenta la red de redes

El año de 1994 ha sido que ha determinado en gran parte la corta historia del Internet. Pronto el Internet será conocido por todos y su acceso será algo tan común como ver la televisión. Millones de computadoras compartirán un océano de información. Ya existe un gran número de compañías ofreciendo al público acceso gratis al Internet.<sup>9</sup> El esfuerzo se concentra ahora en crear servicios que faciliten el acceso al inmenso mar de información.

---

<sup>5</sup> Sobre datos de estadística del Internet ver: <http://www.internews.com>, <http://www.iab.com>, <http://www.webreference.com/statistics.html>

<sup>6</sup> En esta investigación se ha revisado varios grupos de discusión acerca de derecho informático, como por ejemplo en la dirección electrónica del internet <http://www.about.com>

<sup>7</sup> Véase el Semanario IUSRISLEX, editado por abogados españoles en <http://www.abogonet.net>

<sup>8</sup> Revista Discovery, "Maravillas de la web", págs.16-17, julio 2000.

<sup>9</sup> En Ecuador aún no se ha dado este caso, pero en otros países de Latinoamérica, Colombia o Chile, una persona puede obtener de manera gratuita el servicio de Internet. Véase: <http://www.tutopia.com>

### **1.3.- El Derecho Informático.-**

---

La Informática está presente en todos los órdenes de nuestra realidad, en el sistema financiero, en el campo militar, en el comercio, en las telecomunicaciones, en las ciencias exactas, en las ciencias humanas, en la educación, en los medios de comunicación y también ha entrado a revolucionar la ciencia del Derecho.

Para el doctor Elías Gustavino, la Informática es “ el tratamiento automático de la información a través de elaboradores electrónicos basados en las reglas de la cibernética.”<sup>10</sup> Define además a esta última disciplina como la “ ciencia que estudia los sistemas de control y especialmente de autocontrol de organismos y máquinas. A su vez, cuando los datos obtenidos de esta manera se transmiten a distancia, surge la teleinformática o telemática (telecomunicaciones e informática.)”<sup>11</sup>

Antes de conceptualizar que es y de que se encarga la rama del Derecho conocida como Derecho Informático, trataremos de dar una breve explicación a lo que se denomina como Informática Jurídica.

En primera instancia, la relación de las ciencias informáticas relacionadas con la ciencia jurídica se ha dado en lo que se denomina como la Informática Jurídica, entendiéndose como tal, el aporte que se circunscribe al aspecto instrumental de la Informática al servicio del Derecho.

Se conceptualiza a la Informática Jurídica como una ciencia que estudia la utilización de tecnologías informáticas, en el área de las ciencias jurídicas.<sup>12</sup> Por tanto esta ciencia está muy relacionada con el ámbito informático antes que con el Derecho.

El Doctor Pablo Yáñez, en el Primer Encuentro de Informática y Derecho, realizado en Quito-Ecuador en el mes de julio del 2.000, define a la Informática Jurídica como la aplicación de las técnicas informáticas que permiten adoptar herramientas de solución a los quehaceres en el mundo jurídico.

La informática Jurídica según Ricardo Guibourg y otros,<sup>13</sup> se divide en :

1.- La Informática Jurídica de gestión u ofimática.- Consiste en funciones de colaboración técnica y administrativa en las tareas jurídicas, que a su vez se subdivide en:

- Informática Registral,
- Informática Notarial,
- Gestión de estudios jurídicos<sup>14</sup>,
- Informática Legislativa, e
- Informática de Investigación.

2) La Informática Jurídica documental o de las fuentes del Derecho. Esta disciplina se encarga de ordenar y recopilar leyes, acuerdos, decretos, ordenanzas, otras normas jurídicas, jurisprudencia y doctrina. Permite el ingreso, archivo y recuperación de datos de interés para la ciencia jurídica. Es menester acotar que este fue el primer aspecto de la relación entre la Informática y del Derecho, de allí surgieron en la década de 1940 y 1950 los términos como Jurimetría, Juscibernética.

De gran ayuda para el juez, el abogado y para toda persona que se interese por conocer la ley, pues permiten el ahorro de tiempo en la búsqueda de las miles de normas jurídicas vigentes en la República.<sup>15</sup>

---

<sup>10</sup> GUSTAVINO, Elías. “Responsabilidad civil y otros problemas jurídicos de la computación”, pág.25.

<sup>11</sup> Ob.Cit., pág.19.

<sup>12</sup> Es conveniente remitirnos al pensamiento de Vittorio Frosini, “ Informática y Derecho”, Ed.Temis, 1996.

<sup>13</sup> GUIBOURG, Ricardo y otros., “Manual de Informática Jurídica”, Ed. Astrea, 1996, Bns.Ars.Argentina.

<sup>14</sup> Ejemplo de ello es el proyecto de modernización de la Justicia ecuatoriana, auspiciado por PROJUSTICIA y el Banco Interamericano de Desarrollo ( BID) en 26 juzgados en la República.

<sup>15</sup> En Ecuador, hay varias empresas privadas que ofrecen este tipo de servicios, como Lexis S.A., Ediciones Legales, Pudeleco, entre otras.

Juristas, legisladores, abogados y personas que se interesan por el fenómeno de la Informática y su vínculo con el Derecho, en los países como Estados Unidos de América, los países pertenecientes a la Comunidad Económica Europea y Japón en la década de 1960 y 1970, empezaron a utilizar el término de Derecho Informático.

3) La Informática Jurídica Decisional.- Estudia la posibilidad de que los ordenadores a través de sistemas expertos puedan llegar a tomar decisiones, sentencia y fallos. Punto que despierta polémica por que dejaría al Juez, al ser humano relegado por un ordenador, lo que daría paso a la aplicación de la Inteligencia Artificial.

### **1.3.1- Concepto de Derecho Informático**

El Derecho Informático es una ciencia que “ trata la relación Derecho e Informática desde el punto de vista de normas legales, doctrina y jurisprudencia, que van a establecer, a regular las acciones, procesos, aplicaciones, relaciones jurídicas, en su complejidad, de la informática.”<sup>16</sup>

Para Perez Luño<sup>17</sup>, “Derecho Informático o Derecho de la Informática estudia una materia inequívocamente jurídica, conformada por el sector normativo de los sistemas jurídicos contemporáneos integrados por el conjunto de disposiciones dirigido a la regulación de las nuevas tecnologías de la información y de la comunicación, es decir de la informática y de la telemática”.

En estos momentos se discute sobre la autonomía del Derecho Informático dentro de las Ciencias Jurídicas, hay autores como Ricardo Guibourg<sup>18</sup> que argumentan que el Derecho Informático se nutre de otras ciencias jurídicas, así por ejemplo al estudiar los contratos informáticos, la protección del software y las transferencias de fondos por vías electrónicas se relaciona con derecho comercial, el valor probatorio de los documentos electrónicos, con el derecho procesal civil , la protección de datos personales con derecho civil y derecho constitucional, los delitos informáticos con derecho penal. De esta forma el Derecho Informático no aparece como una nueva rama semejante a las anteriores, sino el producto de una nueva forma de aglutinar los problemas.

Para otros autores, la autonomía del derecho informático se manifiesta por la generación de cambios en la sociedad que luego son reglados a través de la normativa jurídica. El fenómeno de la informática, como hemos analizado en líneas anteriores se torna inusual, y el cambio que está produciendo y producirá hará que el Derecho Informático constituya en pocos años una rama autónoma del derecho.

Nuestra opinión al respecto se fundamenta en lo siguiente: La informática trastoca varias concepciones en el derecho, como hasta ahora éste es concebido. El comercio electrónico, por ejemplo, traerá más de un problema al intentar fijar el domicilio del comprador, si este realiza la transacción desde un ordenador móvil, conectado vía satélite con el Internet. El delito informático, tema de nuestra investigación, puede ser cometido por menores de edad, inimputables en las legislaciones penales de varios países iberoamericanos. Por lo tanto, el Derecho Informático deberá realizar el estudio particularizado de estos y de otros problemas que se suscitan y se suscitarán por la utilización de las nuevas tecnologías en la sociedad de principios del Siglo XXI y de esa forma podrá ser analizado como realidad científica en las universidades ecuatorianas y como un nuevo ordenamiento jurídico en el que se incurrirán entre otras, la ley de comercio electrónico, el derecho notarial electrónico, el derecho tributario electrónico y el derecho penal informático.

Hay varias universidades en el globo que tienen en sus programas de estudios cátedras como: Informática Jurídica, Derecho Informático, e Institutos de Investigación científica tales como el Instituto para el Derecho y la Informática de la Universidad de Erlangen - Alemania, el Instituto de Informática Jurídica de la Universidad del Salvador en Argentina, Centro de Investigaciones para el Derecho y la Informática de la Universidad de Viena - Austria, el Centro de Informática Jurídica

<sup>16</sup> PEÑARANDA QUINTERO H., “La informática Jurídica y el Derecho Informático”, Revista Electrónica de Derecho Informático, en <http://publicaciones.derecho.org.redi>.

<sup>17</sup> PEREZ LUÑO, Antonio, “ Manual de Informática y Derecho, ed.Ariel, Barcelona, 1996, pág.18.

<sup>18</sup> GUIBORG, Ricardo y otros, Ob.Cit., pág. 220

de la Facultad de Derecho Pío Nono en Santiago de Chile - Chile, el Instituto Español de Informática y Derecho de la Universidad Complutense de Madrid - España, El Instituto de Informática Jurídica de la Universidad Pontificia de Comillas - España, El Instituto para la Ley del Ciberespacio de la Universidad de Georgetown - EUA, Law and Technology de la Escuela de Leyes de la Universidad de Stanford - EUA., El Instituto de Investigaciones y estudios para el tratamiento de la Informática Jurídica de la Universidad de Montpellier-Francia, entre otros varios Institutos y dependencias universitarias que trabajan en el área de la investigación jurídica relacionada a la Informática.

En nuestro país no se han dado pasos en firme para integrar al programa de estudios de las universidades ecuatorianas la cátedra de Informática Jurídica o de Derecho Informático, de esta forma no existen estudios referentes a las nuevas relaciones que surgen del desarrollo de las nuevas tecnologías, no se realiza investigaciones que den como fruto ciencia y doctrina jurídicas que expliquen la irrupción del fenómeno informático en el Derecho.

### **1.3.2.- Particularidades.**

El Derecho Informático se nutre del derecho público y del derecho privado, debido a que su normativa tiene que ver con el valor probatorio de los documentos electrónicos (derecho público - procesal), delitos informáticos (derecho público - penal), los contratos informáticos (derecho privado - comercial), la concesión de nombres de dominio en el internet (derecho privado - comercial).

También se puede hablar que el Derecho Informático tiene la particularidad de constituirse en un integrador de normas jurídicas que tengan estrecha relación con la normativa de todos los países de mundo. Esta particularidad tiene relación con el derecho comparado a fin de concebir un ordenamiento jurídico que esté acorde a la normativa internacional, debido a que muchos de los tópicos que enfoca el Derecho Informático tendrán que ver con la aplicación de leyes en distintos países del orbe.

La compra-venta realizada a través del comercio electrónico puede ser realizada por un comprador que se sitúe en el Ecuador y un vendedor que se encuentre en Filipinas, el producto es entregado en Francia; hagamos una suposición y digamos que el objeto materia de la compra-venta tenía vicios ocultos, el comprador ecuatoriano ¿ Ante quién deberá formular su reclamación? ¿ Bajo qué jurisdicción se sometieron los comparecientes, si fue un negocio realizado por medio del Internet. ? Este es un solo ejemplo en el observamos que las normas jurídicas integrantes del Derecho Informático deberán tener un carácter internacional.

El Derecho Informático estudia los siguientes aspectos:

La propiedad intelectual

- a.1) El sistema de patentes y marcas
- a.2) La protección legal del software
- a.3) Responsabilidad civil por competencia desleal.
- a.4) Principios Generales del Derecho.

Todos estos temas se encuentran insertos en la legislación de la República del Ecuador en la Ley de Propiedad Intelectual, publicada en el Registro Oficial No.320, del 19 de mayo de 1998.

- a) Los contratos informáticos.- Contratos que se caracterizan por ser catalogados como de adhesión, ya que las cláusulas son escritas por una de las partes, generalmente aquella parte que ofrece servicios de suministro y venta de ordenadores, de mantenimiento de tales equipos, o del proveedor del servicio de Internet.
- b) Los nombres de dominio en el Internet.- Se entiende por tales la concesión o compra de las direcciones en las que una persona puede encontrar información en el Internet. Nos referimos a la serie de caracteres que se colocan en las búsquedas de los programas de exploración de internet tales como Netscape o Explorer que vincula una serie de caracteres con direcciones de IP (Protocolo de Internet).
- c) El valor probatorio de los documentos informáticos.- Tiene que ver con la normativa procesal en la que se analiza cual es el valor de documentos que son originados en

- sistemas electrónicos tales como el Internet, como el fax, con computadoras Palm como el envío de información a través de medios de soporte magnético o disquetes.<sup>19</sup>
- d) Transferencias electrónicas de fondos.- Normativa jurídica que tiene que ver con uso de sistemas de cajeros automáticos, transferencias domiciliarias, tarjetas inteligentes.
  - e) Flujos internacionales de datos.- Se refiere a "todo tipo de transmisión, salida, o emisión de información a través de los Estados, tratada o destinada a ser tratada por computadores o almacenadas en medios magnéticos, o capturada o enviada por satélites, o transportada en cualquier tipo de soporte y destinada a su consulta, procesamiento o almacenamiento."<sup>20</sup>
  - f) Los Delitos Informáticos.- Tema que será analizado en los siguientes capítulos del presente trabajo de investigación. La intimidad y los datos personales.- El avance de la Informática en la recopilación de datos de ciudadanos en el mundo a generado un gran problema.

Para nosotros no es desconocido las bases de datos que se han recopilado en las entidades del Sistema Financiero Nacional, en donde se recogen los nombres, apellidos, direcciones, patrimonio, edad y muchas otras informaciones de millones de ecuatorianos.

En el Registro de la Propiedad del Cantón Quito-Ecuador se recogen de igual manera los nombres de los propietarios de todos los bienes inmuebles de esa circunscripción territorial. Nos preguntamos bajo que parámetros esas bases de datos tomadas como ejemplo pueden lesionar los derechos de los ciudadanos, por cuanto esa información es susceptible de copiarla, borrarla, transmitirla, difundirla y compararla.

Sobre el punto anterior, desarrollaremos en el siguiente capítulo todo lo que concierne al Derecho a la privacidad, o a la intimidad, de esa manera ahondaremos más en el estudio de este tema de investigación del Derecho Informático.

### **1.3.3.- Hacia un Derecho Penal Informático.**

Se denomina Derecho Penal Informático, al conjunto de normas de carácter punitivo que penan las actividades ilícitas cometidas a través de las nuevas tecnologías informáticas.

En el ámbito de estudio del Derecho Penal Informático está relacionado con los siguientes ilícitos:

- a) Descubrimiento y revelación de secretos: accesos, utilización o modificación de datos.
- b) Apropiación indebida de secretos industriales.
- c) Apropiación indebida de claves de acceso, tarjetas de crédito o débito.
- d) Estafas informáticas.
- e) Daños a datos o programas electrónicos.
- f) Producción de virus, gusanos, bombas lógicas, u otras programas que dañen, borren o alteren información electrónica.

El Derecho Penal Informático no constituye, un nuevo ordenamiento jurídico diferente a la normativa penal actual, pero deberá adaptarse a las novísimas actividades desarrolladas por el uso y manejo de la Informática y de la Telemática.

## **2.- Concepto de Delito Informático.-**

Con el desarrollo de la tecnología informática y telemática, se han planteado una serie de nuevos fenómenos sociales fruto de esa explosiva expansión.

Los problemas se evidencian en la sociedad y se ven reflejados claramente en el uso y abuso de la tecnología informática, por ello aparecen conductas que son claramente ilegales y nocivas para el mantenimiento de la paz y tranquilidad social.

<sup>19</sup> La Superintendencia de Bancos del Ecuador, recibe el balance diario de las Instituciones del Sistema Financiero Nacional a través del Internet y/o medios de soporte magnéticos como disquetes. El Servicio de Rentas Internas y el Consejo Nacional de Sustancias Psicoactivas y Estupefacientes también reciben información de Bancos y Financieras por medios electrónicos.

<sup>20</sup> GUIBORG, Ricardo y otros, Ob.Cit., 286.

De allí que para proseguir con nuestra investigación es necesario conceptualizar al delito informático y luego definirlo.

El delito informático se refiere a actividades ilícitas que han sido, en un principio, tipificadas en las normas penales tradicionales, de estafa, falsificación, hurto o robo.

El desarrollo de la Informática, como hemos reseñado en este capítulo, ha creado una infinidad de posibilidades de mal uso o abuso de los ordenadores, en consecuencia ha provocado que en las universidades y centros de educación superior se estudien e investiguen estos hechos y se proceda a plantear una tipificación nueva de normas penales para proteger y precautelar los intereses de la sociedad.

En el Primer Encuentro de Derecho e Informática desarrollado en Quito-Ecuador, en julio del año 2.000<sup>21</sup>, el doctor Julio Téllez Valdés señaló 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, (se refiere a México) al igual que en otros muchos no ha sido objeto de tipificación aún.

Si bien es cierto que en la legislación penal ecuatoriana no existe norma alguna que se refiera a los delitos informáticos, trataremos de conceptualizarlos a través de las opiniones de tratadistas vinculados al Derecho Informático.

La delincuencia informática es conceptualizada por el doctor Miguel Gómez Peralas como “ el conjunto de comportamientos dignos de reproche penal que tienen por instrumento o por objeto a los sistemas o elementos de técnica informática, o que están en relación significativa con ésta, pudiendo presentar múltiples formas de lesión de variados bienes jurídicos.”<sup>22</sup>

El doctor Rogelio Baón Ramírez, señala que la criminalidad informática es la “... realización de un tipo de actividades que, reuniendo los requisitos que delimitan el concepto de delito, sean llevados a cabo utilizando un elemento informático (mero instrumento del crimen) o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software (en éste caso lo informático es finalidad).”<sup>23</sup>

### **3.- Definición de delito informático.-**

El profesor Miguel Angel Davarra Rodríguez en su obra Manual de Derecho Informático, define al delito informático como, “ la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático y/o telemático, o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software.”<sup>24</sup>

El doctor 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".<sup>25</sup>

---

<sup>21</sup> El Primer Encuentro de Derecho e Informática se realizó los días 27 y 28 de julio del año 2.000 en el campus de la Escuela Politécnica del Ejército ecuatoriano ( ESPE), con la presencia de exponentes de toda América Latina.

<sup>22</sup> GÓMEZ PERALS, Miguel. “ Los Delitos Informáticos en el derecho español ”, Informática y Derecho No.4, UNED, centro Regional de Extremadura, III Congreso Iberoamericano de Informática y Derecho, 21-25 de septiembre de 1992, Mérida, 1994, Editorial Aranzadi, pág. 481 a 489.

<sup>23</sup> BAÓN RAMÍREZ, Rogelio. “Visión General de la Informática en el Derecho Penal” , Cuadernos de Derecho Judicial, Escuela Judicial/Consejo General del Poder Judicial, Madrid, págs.78-95

<sup>24</sup> DAVARRA RODRÍGUEZ, Miguel Angel., “ Manual de Derecho Informático”, ed. Aranzadi, Pamplona, 1997, págs. 285-326.

<sup>25</sup> FERNÁNDEZ CALVO, Rafael, “ El tratamiento del llamado Delito Informático” en el proyecto de Ley Orgánica del Código Penal: Reflexiones y propuestas de la CLI ( Comisión de Libertades e Informática),

La doctora María de la Luz Lima explica 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".<sup>26</sup>

Compartimos la noción de delito informático efectuada por el doctor Julio Téllez Valdés<sup>27</sup>, quien 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 utiliza el ordenador, como instrumento o fin, tales como "delitos informáticos", "delitos electrónicos", "delitos relacionados con las computadoras", "crímenes por computadora" " ciber crímenes" " criminalidad cibernética."

De acuerdo y en relación a lo expresado en párrafos anteriores, en la presente investigación se entenderán como "delitos informáticos" todas aquellas conductas ilícitas que deben ser tipificadas en los códigos penales, en las que el ser humano hace uso indebido de cualquier medio informático o relacionado con el desarrollo de nuevas tecnologías informáticas.

---

Informática y Derecho No.12, 13, 14, 15. UNED, Centro Regional de Extremadura, Mérida, 1996, págs. 1149 a 1162.

<sup>26</sup> LIMA DE LA LUZ, María., "Delitos electrónicos" en Criminalia, Academia Mexicana de Ciencias Penales, Ed. Porruá., No.1-6 Año L, Enero - Junio 1984, pág.100.

<sup>27</sup> TÉLLEZ VALDÉS, Julio., " Los delitos informáticos. Situación en México, Informática y Derecho" No.9, 10 y 11, UNED, Centro Regional de Extremadura, Mérida, 1996, pág. 461-474.

# **CAPITULO II: MARCO JURÍDICO Y CARACTERES DE LOS DELITOS INFORMÁTICOS**

## **1. - Principio de legalidad y reserva.-**

Recordemos el aforismo latino Nullum crimen, nulla pena, sine crimen. No hay delito ni pena sin que una ley los haya establecido de manera previa. De tal forma que la ley penal “ es la única forma de norma jurídica que puede crear delitos y establecer pena, la ley penal no puede operar de forma retroactiva, y la ley penal, al crear los delitos y las penas, debe referirse directamente a los hechos que constituyen aquellos y a su naturaleza y límites de éstas”.<sup>28</sup>

Los principios de legalidad y reserva se han recogido tanto en la Constitución Política Vigente como en el Código Penal y en el Código de Procedimiento Penal, de tal forma que transcribiremos las normas anotadas:

### **CONSTITUCIÓN POLITICA DE LA REPÚBLICA DEL ECUADOR<sup>29</sup>**

*Art. 24. - Para asegurar el debido proceso deberán observarse las siguientes garantías básicas, sin menoscabo de otras que establezcan la Constitución, los instrumentos internacionales, las leyes o la jurisprudencia:*

*1. Nadie podrá ser juzgado por un acto u omisión que al momento de cometerse no esté legalmente tipificado como infracción penal, administrativa o de otra naturaleza, ni se le aplicará una sanción no prevista en la Constitución o la ley. Tampoco se podrá juzgar a una persona sino conforme a las leyes preexistentes, con observancia del trámite propio de cada procedimiento.*

*3. Las leyes establecerán la debida proporcionalidad entre infracciones y sanciones. Determinará también sanciones alternativas a las penas de privación de la libertad, de conformidad con la naturaleza de cada caso, la personalidad del infractor y la reinserción social del sentenciado.*

Las disposiciones constitucionales anotadas están en relación con las normas penales que se señalan a continuación.

### **Código Penal de la República del Ecuador<sup>30</sup>:**

*Art. 1. - Leyes penales son todas las que contienen algún precepto sancionado con la amenaza de una pena.*

*Art. 2. - Nadie puede ser reprimido por un acto que no se halle expresamente declarado infracción por la ley penal, ni sufrir una pena que no esté en ella establecida.*

*La infracción ha de ser declarada, y la pena establecida, con anterioridad al acto.*

<sup>28</sup> Etcheberry, Alfredo, “ Curso de Derecho Penal” Ed. Jurídica de Chile, 1976, págs.47 y siguientes., Citado por Jijena Leiva Renato, “ Chile, la protección penal de la intimidad y el delito informático”, Ed.Jurídica de Chile, 1994, pág.72.

<sup>29</sup> Ediciones Legales, Sistema de Recopilación de normas jurídicas de la República del Ecuador, Quito, 2.000

<sup>30</sup> Ob.Cit. Ediciones Legales.

*Deja de ser punible un acto si una ley posterior a su ejecución lo suprime del número de las infracciones; y, si ha mediado ya sentencia condenatoria, quedará extinguida la pena, haya o no comenzado a cumplirse.*

*Si la pena establecida al tiempo de la sentencia difiere de la que regía cuando se cometió la infracción, se aplicará la menos rigurosa.*

*En general, todas las leyes posteriores sobre los efectos y extinción de las acciones y de las penas se aplicarán en lo que sean favorables a los infractores, aunque exista sentencia ejecutoriada.*

El artículo 219 del precitado cuerpo legal existe una norma en relación con las anteriores.

*Art. 219. - Antes de iniciar el sumario, el Juez está obligado a examinar si el hecho está previsto como delito en la Ley Penal, bajo prevención de pagar indemnización de daños y perjuicios, independientemente de la sanción penal a que hubiere lugar*

### **Código de Procedimiento Penal de la República del Ecuador<sup>31</sup>:**

*Art. 158. - Nadie puede ser reprimido por un acto que no se halle expresamente declarado como infracción por la Ley Penal, ni sufrir una pena que no esté en ella establecida.*

*La infracción ha de ser declarada y la pena establecida con anterioridad al acto.*

*Deja de ser punible un acto si una Ley posterior a su ejecución lo suprime del número de las infracciones; y, si ha mediado ya sentencia condenatoria, quedará extinguida la pena, haya o no comenzado a cumplirse.*

*Si la pena establecida al tiempo de la sentencia difiere de la que regía cuando se cometió la infracción, se aplicará la menos rigurosa.*

*En general todas las leyes posteriores sobre los efectos y extinción de las acciones y de las penas se aplicarán en lo que sean favorables a los infractores, aunque exista sentencia ejecutoriada.*

### **Código de Menores de la República del Ecuador:**

*Art. 165, inc. 2. - Se entenderá que existe infracción cuando el menor realice un acto que se encuentre tipificado en las leyes penales. Ningún menor podrá ser declarado autor o partícipe de una infracción que no esté expresamente consagrada en la Ley Penal vigente al momento en que esta se cometió.*

Una vez revisadas las normas jurídicas, deducimos que de no haber norma penal que sancione las conductas antijurídicas cometidas utilizando un ordenador como fin o medio para cometer ilícitos denominados como informáticos, no habría sanción penal de un sinnúmero de conductas antijurídicas y atentatorias de la paz y seguridad social, de tal forma que aquellas conductas quedarían en completa impunidad<sup>32</sup>, de allí la urgencia de delimitar cuál o cuales son los bienes

<sup>31</sup> Ob.Cit. Ediciones Legales.

<sup>32</sup> Transcribimos dos fallos expedidos por la Corte Suprema de Justicia del Ecuador sobre el tema tratado en este numeral.

**12-XII-90 (Prontuario 3, p. 369)** “Según la ley anterior el consumo de estupefacientes y consecuentemente la tenencia con este fin exclusivo no era considerado como delito, y así lo indica el artículo 26. La infracción fue cometida cuando estaba vigente la ley anterior, consecuentemente de acuerdo con los incisos cuarto y quinto del Art. 2 del Código Penal ... el acusado no cometió infracción.”

**- 17-VI-93 (GJ, S. XV, No. 2, p. 27)**

“El Código Penal en su Art. 2, incisos 2o. y 4o., dispone que la pena ha de ser establecida con anterioridad al acto, y si la pena establecida al tiempo de la sentencia difiere de la que regía cuando se cometió la infracción, se aplicará la menos rigurosa; de otro lado, es evidente que con relación a la Ley de Control y

jurídicos a protegerse penalmente, bienes jurídicos que serán motivo del siguiente análisis en esta investigación.

## **2. Bienes jurídicos a ser protegidos.**

Antes de describir cuales son los bienes jurídicos que se lesionan por las conductas ilegales denominadas como delitos informáticos, debemos apoyarnos en las doctrinas de los tratadistas del Derecho Penal para entender el concepto de los bienes jurídicos.

Para el tratadista Von Liszt todos los bienes jurídicos son "...intereses vitales, interés del individuo o de la comunidad. No es el ordenamiento jurídico lo que genera el interés, sino la vida; pero la protección jurídica eleva el interés vital a bien jurídico. Los intereses vitales deben ser indispensables para la convivencia comunitaria luego de lo cual y como consecuencia de ello serán protegidos normativamente bajo juicios de valor positivo."<sup>33</sup>

Para el doctor Francisco Muñoz Conde "los bienes jurídicos son aquellos presupuestos que la persona necesita para su autorealización y el desarrollo de su personalidad en la vida social"<sup>34</sup>

Los bienes jurídicos en el Derecho Penal son muy importantes puesto que determinan cuales son los intereses que la sociedad considera imprescindibles proteger.

El legislador a través de la norma penal otorga la protección jurídica a los bienes referidos, norma que traerá la amenaza y la imposición de la pena.

El bien jurídico puede presentarse como "objeto de protección de la ley o como objeto de ataque contra el que se dirige el delito y no debe confundirse con el objeto de la acción que pertenece al mundo de lo sensible. Siguiendo el ejemplo más común: en el hurto el objeto de la acción es la cosa sustraída; el objeto de la protección, la propiedad."<sup>35</sup>

A continuación revisemos qué tipo de bienes jurídicos se lesionan por el desarrollo de las ciencias informáticas y las Nuevas Tecnologías.

### **2.1.- Derecho a la intimidad.**

Como habíamos explicado en el Capítulo I de esta investigación, la Informática se ha constituido en un tema de principal importancia en todos los campos de la actividad de la vida de la humanidad en los últimos decenios del siglo XX y los primeros años del Siglo XXI.

Las ventajas que nos han traído el desarrollo de las Ciencias Informáticas y la de las Nuevas Tecnologías han sido cuantiosas. Solo es necesario observar el desarrollo de la exploración espacial, y las fabulosas imágenes que nos llegan desde los más lejanos rincones del Universo, el desarrollo de equipos de exploración médica que permiten un diagnóstico con mucha mayor rapidez y confiabilidad, el diseño de obras de ingeniería de la más variada índole, el teletrabajo, el comercio electrónico, para nombrar solo algunas de las múltiples aplicaciones en la sociedad actual.

---

*Fiscalización del Tráfico de Estupefacientes y Sustancias Psicotrópicas, la nueva Ley sobre Sustancias Estupefacientes y Psicotrópicas promulgada el 17 de septiembre de 1990 vino a establecer penas más severas para los delitos de esa naturaleza; por tanto, habiéndose cometido los hechos el día 8 de febrero de 1990 ... y levantándose el auto cabeza de proceso a los quince días del mes de febrero del mismo año, es aplicable en este caso la ley mencionada en primer lugar"*

<sup>33</sup> Citando a VON LISZT Frank, BUSTOS RAMIREZ, Juan. & VALENZUELA BEJAS, Manuel.

DERECHO PENAL LATINOAMERICANO COMPARADO- PARTE GENERAL, pág. 130-131, Buenos Aires, 1981.

<sup>34</sup> MUÑOZ CONDE, Francisco & GARCÍA ARAN, Mercedes. "MANUAL DE DERECHO PENAL", pág.54.

<sup>35</sup> ENCICLOPEDIA JURÍDICA OMEBA, Tomo II, pag. 189.

De la igual forma, el desarrollo de la Informática y de las Nuevas Tecnologías, entre la cuales podemos anotar las telecomunicaciones y la telemática, y su mal utilización y aprovechamiento traen como secuela que se cometan nuevos tipos de atentados a los bienes jurídicos dignos de protección penal.

Pero veamos como responde la ciencia jurídica ante éstos hechos, para ello es necesario recoger el pensamiento del profesor Vittorio Frosini<sup>36</sup> quien realiza una breve historia del nacimiento del derecho a la intimidad.

A raíz de un ensayo titulado como "The right to privacy," publicado en los Estados Unidos de América a fines del Siglo XIX en el que dos abogados norteamericanos explican que todo individuo debe ser dejado en paz, tiene derecho a proteger su soledad, su vida íntima, del mismo modo a proteger su vida privada. Este concepto ha ido evolucionando y ahora no solamente se refiere a las relaciones de los individuos particulares, sino también a las relaciones entre el ciudadano y la administración pública.

El tratamiento automatizado de datos ha hecho que en estas últimas décadas la información se difunda con mucha mayor velocidad que en épocas anteriores de la humanidad. Es así que en "1865 se necesitaron 12 días para conocer en Europa el asesinato de Lincoln, Presidente de los Estados Unidos. Cien años después - 22 de noviembre de 1963- sobraron 12 minutos para que se difundiera el asesinato de John F. Kennedy."<sup>37</sup> En 1990 el mundo miró atónito, por televisión abierta, los bombardeos en Bagdad-Irak en la llamada Guerra del Golfo, imágenes que llegaron a nuestros hogares de forma inmediata, sin mediar tan solo un segundo entre la realidad y las imágenes que observamos.

Veamos ahora el alcance del concepto del derecho a la información, que en opinión del Doctor Frosini tiene "doble significado: es el derecho que todos tenemos de ser informados de lo que sucede y que puede interesarnos; y es también el derecho, atribuido en particular a los periodistas, a los reporteros gráficos, a los operadores de televisión, de informar a los lectores y a los espectadores acerca de los acontecimientos. Este derecho, que consiste en la libertad de recoger e intercambiar informaciones, se encuentra reconocido como uno de los derechos humanos en los acuerdos de Helsinki de 1975, suscritos entre los Estados Unidos, la Unión Soviética (ahora Rusia) y los países europeos."<sup>38</sup>

En principio las empresas públicas y privadas recogen datos inherentes a las personas y que son de uso común, como por ejemplo nombres y apellidos, lugar de nacimiento, lugar del domicilio, número de teléfono y otros en razón del trabajo que desempeñamos. Datos como por ejemplo el estado de salud, constituye un dato íntimo y que la doctrina más calificada lo ubica dentro de la categoría de **datos sensibles**, incluyendo dentro de éstos los referidos a las costumbres, hábitos sexuales y creencias religiosas o políticas de una persona.

En el primer grupo de ejemplos dados en el párrafo anterior, cuando los datos personales son puestos a disposición de gran número de personas, como en la guía telefónica, o el padrón electoral, sin que su titular pueda saber o impedir que una vez conocidos, sean libremente difundidos dentro de unos límites de respeto y de convivencia cívicos, la doctrina española<sup>39</sup> los ha denominado "datos públicos", en contraposición a los datos privados, los que se trata de impedir su difusión y de esa forma respetar la voluntad de secreto de su titular, siendo reguladas las situaciones o circunstancias en las cuales el individuo debe suministrarlos.

Frente a estas situaciones, el derecho a la libertad informática se erige como un medio de control y protección de estas dos clases o categorías de datos, se encuentren informatizados o no, en otras palabras, está referida a brindar la protección de los datos de la vida privada y de la vida íntima, que se encuentren almacenados en archivos automáticos o manuales.

Definido como ha sido el derecho a la libertad informática, se debe señalar que el mismo guarda estrecha relación con las más recientes concepciones de los derechos a la intimidad y a la

---

<sup>36</sup> Ob. Cit., págs.65 y ss.

<sup>37</sup> GASTALDI, Italo, " El hombre, un misterio" Instituto Superior Salesiano, Quito, 1994, pág., 11.

<sup>38</sup> FROSINI, Ob.Cit. Pág.66.

<sup>39</sup> DAVARRA RODRIGUEZ, Miguel, " Manual de Derecho Informático " Ed.Aranzadi, Pamplona, pág.55

privacidad, cuyas nociones han evolucionado con el tiempo, de manera que las normativas primigéneas de protección de la intimidad fueron muy limitadas con relación al contenido material de los mencionados derechos y que en la actualidad, el legislador debe tomar muy en cuenta para analizar y crear la normativa jurídica que ha de regular las relaciones que se desprenden de la utilización de la informática y de las Nuevas Tecnologías.

Sobre el derecho a la intimidad, la doctrina y jurisprudencia española, han trasladado el contenido esencial del referido derecho desde la facultad de aislamiento (*ius solitudinis*) al poder de control sobre las informaciones relevantes para cada sujeto, observándose entonces, una evolución positiva de este derecho configurado originalmente en sentido negativo.

Para los españoles, el derecho a la intimidad presenta hoy un doble aspecto<sup>40</sup>: por un lado, un derecho de defensa de la persona y por el otro, el control de las informaciones que la afectan, entendido éste como un derecho de intervención.

Nos parece interesante comentar la doctrina española, incluye dentro de algunos aspectos específicos de la intimidad el derecho sobre el propio cuerpo, la ampliación del concepto entorno familiar y el derecho al olvido.

Con referencia al derecho al olvido, éste consiste en la facultad que tiene un individuo o su familia de que no se traigan al presente hechos verídicos realizados en el pasado, deshonorosos o no y que por el transcurso del tiempo no son conocidos socialmente, pero que de divulgarse puedan aparejarle el descrédito público. El derecho al olvido, en el caso del tratamiento de los datos personales, implica que éstos tengan un período de vida útil, después del cual su permanencia en los archivos manuales o automatizados podría resultar lesiva y estigmatizadora del individuo, obstaculizando su inserción en la sociedad y el desarrollo pleno de su personalidad.

Reafirmamos que desarrollo vertiginoso de las nuevas tecnologías amenaza invadir espacios antes no conocidos de la intimidad persona, de allí que se pueda hablar de un derecho que regule y proteja la intimidad en materia de tratamiento de la información de índole personal, el cual ha sido denominado "derecho a la libertad informática".

Para algunos autores españoles, como el doctor Davarra y el doctor Pérez Luño, se trata de proteger lo que la doctrina anglosajona denomina "privacy", término castellanizado como "privacidad", que le garantiza al ciudadano el derecho a exigir que permanezca en su esfera interna el resultado del tratamiento de su información personal.

La sustitución del término "intimidad" por "privacidad" ha sido acogida también por el legislador español. Al respecto, en la exposición de motivos de la Ley Orgánica Española de Regulación del tratamiento Automatizado de los Datos de Carácter Personal (LORTAD) No. 5/1992 se señaló que: "la intimidad protege la esfera en que se desarrollan las facetas más singularmente reservadas de la vida de la persona...la privacidad constituye un conjunto más amplio, más global, de facetas de su personalidad que, aisladamente consideradas, pueden carecer de significación intrínseca pero que, coherentemente enlazadas entre sí, arrojan como precipitado un retrato de la personalidad del individuo que éste tiene derecho a mantener reservado....".

Es necesario anotar que la Ley antes nombrada fue sustituida por la Ley Orgánica de Protección de Datos de Carácter Personal 15/99, vigente en España<sup>41</sup>

En consecuencia, las nuevas tecnologías de la información y la comunicación le añaden a la privacidad un elemento nuevo, "la necesidad de proteger al individuo ante la posibilidad de que los datos que se contienen en archivos informáticos diversos, por tanto, fuera del espacio que la persona se mueva, pongan de manifiesto una personalidad determinada, cuyo conocimiento pueda decidir a los demás a tratarla de una manera perjudicial para sus intereses o, en todo caso, de una forma predeterminada"<sup>42</sup>

<sup>40</sup> CARRILLO, Marc, " Los límites a la libertad de prensa en la Constitución Española de 1978", Promociones y Publicaciones Universitarias (PPU) pág.73

<sup>41</sup> Se puede revisar el texto íntegro de la Ley Orgánica de Protección de Datos de Carácter Personal de España ( LOPD), [http://club.telepolis.com/vicenti/ce78/Vicenti/lotc/Vicenti/lloo/lo15\\_99.htm](http://club.telepolis.com/vicenti/ce78/Vicenti/lotc/Vicenti/lloo/lo15_99.htm)

<sup>42</sup> DE CARRERAS SERRA, Luis, " Régimen Jurídico de la Información " Ed.Ariel, Barcelona. pág.82

En la evolución del contenido del derecho a la privacidad a que dentro de éste confluya un conjunto más amplio de espacios de lo individual, que ameritan protección jurídica. Es el caso de los **derechos a la imagen, al nombre y a la voz**.

La Constitución recoge los principios que hemos descrito en este capítulo en los numerales ocho, trece y veintiuno del artículo 23. Numerales que transcribimos:

## **CONSTITUCIÓN POLITICA DE LA REPÚBLICA DEL ECUADOR**

### **Capítulo 2**

#### **DE LOS DERECHOS CIVILES**

*Art. 23. - Sin perjuicio de los derechos establecidos en esta Constitución y en los instrumentos internacionales vigentes, el Estado reconocerá y garantizará a las personas los siguientes: ...*

*8. El derecho a la honra, a la buena reputación y a la intimidad personal y familiar. La ley protegerá el nombre, la imagen y la voz de la persona.*

*13. La inviolabilidad y el secreto de la correspondencia. Esta sólo podrá ser retenida, abierta y examinada en los casos previstos en la ley. Se guardará el secreto de los asuntos ajenos al hecho que motive su examen. El mismo principio se observará con respecto a cualquier otro tipo o forma de comunicación.*

*21. El derecho a guardar reserva sobre sus convicciones políticas y religiosas. Nadie podrá ser obligado a declarar sobre ellas. En ningún caso se podrá utilizar la información personal de terceros sobre sus creencias religiosas y filiación política, ni sobre datos referentes a salud y vida sexual, salvo para satisfacer necesidades de atención médica.*

El derecho a la libertad informática garantiza el nuevo status del individuo de la sociedad digital; asegurando que la información de carácter íntimo o privado del individuo no pueda ser manipulada o transmitida por terceros sin su consentimiento y que sea rectificada, y/o actualizada en los casos que sea necesario.

Como todo bien jurídico, el derecho a la libertad informática requiere de una adecuada tutela que permita su exigibilidad frente al Estado y a terceros que efectúen "tratamiento de datos personales" que restrinjan, menoscaben o lesionen el referido derecho. Como derecho fundamental que constituye, impone la preservación del mismo a toda costa, de forma tal que los poderes públicos y en especial, el legislador y el juez, adopten las medidas necesarias para proteger esa libertad. Ahora bien, el derecho comparado ha demostrado que la libertad informática se protege con la creación de leyes de protección de datos personales y con la constitución de organismos de aplicación y de control de las referidas leyes.

Se puede concluir diciendo que el derecho a comunicar o recibir libremente informaciones o ideas, derecho fundamental en un régimen democrático encuentra como límites el respeto a los demás derechos, entre los cuales figura la intimidad.

### **2.1.2. - Protección penal de la intimidad.**

Recordemos que el concepto de intimidad fue enunciado hace más de cien años, mas ese bien jurídico, la intimidad, era protegido y regulado por las leyes penales solo en referencia a la inviolabilidad domiciliaria y de la correspondencia. Revisemos las normas penales ecuatorianas en cuanto a la protección penal de la intimidad.

#### **Código Penal Ecuatoriano.**

### **Capítulo IV**

#### **DE LOS DELITOS CONTRA LA INVOLABILIDAD DEL DOMICILIO**

*Art. 191. - Los empleados del orden administrativo o judicial, los oficiales de justicia o de policía, los comandantes o agentes de la fuerza pública que, obrando como tales, se hubieren introducido*

en el domicilio de un habitante, contra la voluntad de éste, fuera de los casos previstos y sin las formalidades prescritas por la ley, serán reprimidos con prisión de seis meses a dos años y multa de cuarenta a cien sucres.

Art. 192. - Será reprimido con prisión de un mes a dos años y multa de cuarenta a ochenta sucres, el que sin orden de la autoridad y fuera de los casos en que la ley permite entrar en el domicilio de los particulares, contra la voluntad de éstos, se hubiere introducido en una casa, departamento, pieza o vivienda, habitada por otro, o sus dependencias cercadas, ya por medio de amenazas o violencias, ya por medio de fractura, escalamiento o ganzúas.

Art. 193. - La prisión será de seis meses a cinco años y la multa de ochenta a doscientos sucres, si el hecho ha sido cometido con una orden falsa de la autoridad pública, o con el traje o bajo el nombre de uno de sus agentes o con una de las tres circunstancias siguientes:

Si el acto ha sido ejecutado de noche;

Si ha sido ejecutado por dos o más personas; y,

Si los culpables o alguno de ellos llevaban armas.

Art. 194. - Los culpados de las infracciones previstas en los dos artículos anteriores serán colocados bajo la vigilancia de la autoridad por un tiempo igual al de la condena.

Art. 195. - Será reprimido con prisión de quince días a seis meses y multa de treinta y cinco a ochenta sucres, el que se hubiere introducido, sin el consentimiento del propietario, o del locatario, pero sin violencias o amenazas, en los lugares designados en el Art. 192, y haya sido encontrado en ellos durante la noche.

Art. 196. - En la violación de domicilio se presume que no hay consentimiento del dueño o su encargado cuando no están presentes en el acto que constituya la violación.

## **Capítulo V**

### **DE LOS DELITOS CONTRA LA INVIOLABILIDAD DEL SECRETO**

Art. 197. - Serán reprimidos con prisión de dos meses a un año y multa de cuarenta a cien sucres, los empleados o agentes del Gobierno y los del servicio de estafetas y telégrafos que hubieren abierto o suprimido cartas confiadas al correo, o partes telegráficas, o que hubieren facilitado su apertura o supresión.

Art. 198. - Los que, siendo depositarios de partes telegráficas, hubieren revelado su existencia o contenido, a excepción de los casos en que fueren llamados a declarar en juicio y de aquellos en que la ley les obligue a hacer conocer la existencia o contenido de dichos despachos, serán reprimidos con prisión de quince días a seis meses y multa de cuarenta a ochenta sucres.

Art. 199. - El que hallándose en posesión de una correspondencia no destinada a la publicación, la hiciera publicar, o presentare en juicio sin orden judicial, aunque haya sido dirigida a él, será reprimido con multa de cuarenta a doscientos sucres, si el acto puede causar perjuicio a terceros; a no ser que se trate de correspondencia en que consten obligaciones a favor del tenedor de ella, caso en el que puede presentarse en juicio.

Art. 200. - En la misma pena incurrirá el que, sin ser empleado público, divulgare actuaciones o procedimientos de que haya tenido conocimiento y que, por ley, deben quedar reservados.

Art. 201. - El que teniendo noticia, por razón de su estado u oficio, empleo, profesión o arte, de un secreto cuya divulgación puede causar daño, lo revelare sin causa justa, será reprimido con prisión de seis meses a tres años y multa de cincuenta a quinientos sucres.

Art. 202. - Los que sustrajeren cartas confiadas al correo serán reprimidos con prisión de quince a sesenta días, excepto los padres, maridos o tutores que tomaren las cartas de sus hijos, consortes o pupilos, respectivamente, que se hallen bajo su dependencia.

En nuestro país, el legislador no se ha preocupado por regularizar normas penales que protejan el derecho a la libertad informática, vulnerado por el mal uso de los ordenadores; de igual forma no existen en nuestro país publicados estudios ni investigaciones jurídicas sobre este tema (protección penal del derecho a la libertad informática) y en las Universidades del país apenas hay interés sobre el tema, pese a que la mayoría de países latinoamericanos le han dado la importancia que se merece.

Por tanto, se hace necesario que revisemos las legislaciones de otros países del mundo, así como doctrinas de investigadores de la Ciencia Jurídica para comprender el porqué la violación al derecho a la intimidad exige la existencia de una normativa penal.

### **2.1.3. - Tutela constitucional del bien jurídico denominado "intimidad" en el derecho comparado.<sup>43</sup>**

En el desarrollo de este punto de investigación, hemos creído necesario y conveniente remitirnos en primer lugar al estudio de las constituciones Latinoamericanas ya que se hallan mucho más de acuerdo con la realidad nacional que otras constituciones del mundo.

En varias de las Constituciones Latinoamericanas se evidencian una serie de normas y disposiciones que tienen relación con garantizar el derecho a la libertad o intimidad informática.

Las Constituciones de Colombia (1.991), Argentina (1.994), Perú (1.993), Paraguay (1.992), Nicaragua (1.987), Brasil (1.988), reconocen expresamente el derecho a la libertad informática.

Se observa la ampliación de la esfera de la protección a la vida privada de los individuos, ya que se consagra expresamente la protección: *a la propia imagen* (Honduras, Ecuador, Brasil, Perú), *a la voz* (Ecuador, Perú) y *a la intimidad personal y familiar* (Colombia, Ecuador, Honduras, Perú).

Es evidente que las naciones descritas anteriormente han visto la necesidad de elevar los principios generales relacionados con el derecho a la intimidad a la categoría de normas constitucionales y a facetas del individuo tales como su imagen, su voz, su intimidad personal y familiar, las cuales están expuestas a considerables amenazas y riesgos derivados del tratamiento que permiten la informática y las nuevas tecnologías y que tradicionalmente han sido protegidos por los derechos de la personalidad, lo que obliga, reitero una vez más este criterio, al legislador ecuatoriano a establecer normas específicas y especiales para la tutela de los anteriores derechos, por cuanto resulta insuficiente su protección con la mera consagración de cláusulas generales que consagran el derecho a la vida privada.

Las Constituciones de Brasil y Perú establecen diferencias entre la vida privada de la intimidad, lo cual demuestra el reconocimiento expreso de los ámbitos de lo "íntimo y de lo privado"

El cambio experimentado por el desarrollo de los conceptos jurídicos de intimidad, privacidad y protección de datos ha sido muy diferente en Europa, si lo comparamos con América Latina, desarrollo incipiente caracterizado por esfuerzos aislados y particulares en la evolución principalmente constitucional y presentando un escaso desarrollo legislativo y jurisprudencial.

La experiencia europea, con más de 30 años de evolución legislativa, recoge a través de numerosos principios y normas comunitarias el derecho a la intimidad, dotándola a su vez de numerosas garantías y organismos que velen por la efectividad del mencionado derecho, lo cual reafirma nuestra tesis sobre su independencia y autonomía. Ejemplo de ellos son los siguientes organismos la Agencia de Protección de Datos (España), Tribunal de Protección de Datos y Registrador (Reino Unido), Comisión de Protección de Datos (Austria), Delegados Federales para la Protección de Datos (Alemania), Comisión Nacional de Informática y Libertades (Francia), Inspectorado de Datos (Suecia), Inspección de Registros (Dinamarca)

Revisemos ahora dos Constituciones europeas, la Constitución de Portugal de 1976 y la Española de 1978.

La Constitución Portuguesa en su artículo 35 recoge el principio de libertad informática, consagrando el derecho a conocer, el de acceso y el de rectificación, asimismo establece que la informática no debe ser utilizada para el tratamiento de datos sensibles, es decir, referentes a convicciones políticas o religiosas o a la vida privada, salvo que se trate de datos no identificables con fines estadísticos.

---

<sup>43</sup> Para el desarrollo de este tema nos sirvió de base la página <http://www.justiano.com/constituciones>, en donde se recogen los textos íntegros de decenas de constituciones de América Latina y el mundo

La Constitución Española en su artículo 18.4 establece que: "La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".

Y el artículo 105.b tutela el derecho a la libertad informática al establecer: "El acceso de los ciudadanos a los archivos y registros administrativos, salvo en lo que afecte a la seguridad y defensa del Estado la averiguación de los delitos y la intimidad de la persona".

Con el avance de la tecnología, vemos que a través de Internet y el tráfico de la información, corre riesgo de violarse un derecho más profundo de la persona, o sea su privacidad, como ya lo expresamos anteriormente.

## **2.2. - Derecho a la información.**

---

El derecho a la información tiene "doble significado: es el derecho que todos tenemos de ser informados de lo que sucede y que puede interesarnos; y es también el derecho, atribuido en particular a los periodistas, a los reporteros gráficos, a los operadores de televisión, de informar a los lectores y a los espectadores acerca de los acontecimientos. Este derecho, que consiste en la libertad de recoger e intercambiar informaciones, se encuentra reconocido como uno de los derechos humanos en los acuerdos de Helsinki de 1975, suscritos entre los Estados Unidos, la Unión Soviética y los países europeos."<sup>44</sup>

Frente a estas situaciones, el derecho a la libertad informática se erige como un medio de control y protección de estas dos clases o categorías de datos, se encuentren informatizados o no, en otras palabras, está referida a brindar la protección de los datos de la vida privada y de la vida íntima que se encuentren almacenados en archivos automáticos o manuales.

Por lo anteriormente expuesto, no debe confundirse este derecho a la libertad informática, que es un derecho autónomo e independiente que resguarda estos dos espacios de la vida del individuo, con los derechos a la intimidad y a la privacidad respectivamente.

### **2.2.1. - Protección de datos personales.**

---

En Europa a partir de 1970 aparecen por primera vez consagrados los derechos y a su vez organismos protectores de la intimidad y de la libertad informática. El Convenio 108 del Consejo de Europa, del 28 de enero de 1981 sobre "Protección a las personas con respecto al tratamiento automatizado de datos de carácter personal", se hace uniforme la protección que se otorga a los datos personales que conlleva la tutela al derecho a la intimidad y a la libertad informática.

El desarrollo legislativo por parte de los Estados miembros de la Comunidad Económica Europea, países que en virtud de dicho tratado se obligaron a otorgar protección suficiente y garantías al derecho a la intimidad y a la libertad informática al interior de cada Estado; luego se aprobó la Directiva 95/46 del Parlamento Europeo y del Consejo del 24 de octubre de 1.995<sup>45</sup>, en la que a través de un extenso articulado y considerandos reitera la protección al derecho a la intimidad consagrada en el Convenio Europeo, reforzándola asimismo, con la constitución de organismos especiales que custodian el tratamiento de datos y su difusión entre los Estados miembros o no.

Nuestra investigación está encaminada a interesar a los legisladores, jueces, magistrados, abogados en libre ejercicio y a la comunidad en general, sobre los temas de intimidad y libertad informática, y el sustento jurídico del porque es necesario regularizar el procesamiento o tratamiento de datos automáticos o manuales en el Ecuador.

## **2.3. - Derechos patrimoniales.**

---

<sup>44</sup> FROSINI, Ob.Cit. pág.66.

<sup>45</sup> El texto íntegro de la Directiva 95/46 del Parlamento Europeo y del Consejo del 24 de octubre de 1.995, puede revisarse en la siguiente dirección electrónica: <http://www.onnet.es>

Sin lugar a duda alguna, los delitos informáticos atentan contra los derechos patrimoniales de personas naturales y jurídicas. Este tipo de ilícitos produce enormes ganancias económicas, “ el montante unitario promedio de un fraude informático es 25 a 50 veces superior al conseguido en cualquier otro tipo de delito”<sup>46</sup>

## **2.4. - Seguridad Nacional.**

Con el desarrollo del Internet, la circulación de información no se detiene en las circunscripciones territoriales de un país. De allí surgen una serie de problemas que tendrán injerencia en la soberanía de los estados.

Uno de los objetivos principales de los delincuentes informáticos es el de atentar contra la seguridad nacional de los países, es tan importante el tema que los gobiernos de muchos países desarrollados mantienen dentro de sus organismos de seguridad, departamentos especializados que se dedican a precautelar la seguridad nacional.

## **3. Sujeto activo del delito informático.**

El doctor Julio Téllez Valdés<sup>47</sup> explica que 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.

Algunos tratadistas<sup>48</sup> han denominado a los delitos informáticos como de “cuello blanco” término introducido por primera vez por el criminólogo norteamericano Edwin Sutherland en el año 1943. Sin embargo no estamos de acuerdo en dicha afirmación puesto que en múltiples ocasiones se ha establecido que los delincuentes informáticos muchas veces no necesariamente poseen un alto nivel socio-económico.

Seguimos nuevamente al doctor Téllez Valdés en las características de los sujetos activos de los delitos informáticos:

- a) Poseen importantes conocimientos de informática.
- b) Ocupan lugares estratégicos en su trabajo, en los cuales se maneja información de carácter sensible (se los ha denominado delitos ocupacionales ya que se cometen por la ocupación que se tiene y el acceso al sistema.)
- c) A pesar de las características anteriores debemos tener presente que puede tratarse de personas muy diferentes. No es lo mismo el joven que entra a un sistema informático por curiosidad, por investigar o con la motivación de violar el sistema de seguridad como desafío personal, que el empleado de una institución financiera que desvía fondos de las cuentas de sus clientes.
  
- d) Las opiniones en cuanto a la tipología del delincuente informático se encuentran divididas, ya que algunos dicen que el nivel educacional en el ámbito informático no es indicativo, mientras que otros aducen que son personas inteligentes, motivadas y dispuestas a aceptar el desafío tecnológico.

<sup>46</sup> CAMACHO LOSA, Luis “ El delito informático” citado por: Mogliona y López Delincuencia y fraude informático”, Ed.Jurídica de Chile, 1999,pág.71.

<sup>47</sup> TELLEZ VALDEZ, Julio., Ob.Cit., pág.83

<sup>48</sup> GUIBOURG y otros. Ob.Cit.pág.273

## **4. Sujeto pasivo del delito informático.**

Respecto del sujeto pasivo, queda claro que cualquier persona física o jurídica puede ser objeto de alguna de las actividades ilícitas y antijurídicas que se denominan delito informático.

Para entrar en la tipología de sujeto pasivo debe cumplirse con una condición relevante, como es la de ser titular de información de carácter privado y confidencial en formato digital o almacenado en un medio informático. Incluso puede darse el caso de tener información importante pero que no se encuentra en formato digital, o aún estando en formato digital el despojo de se realiza por la fuerza física. En ambos supuestos no puede afirmarse la existencia de un sujeto pasivo de delito informático, sino simplemente de un robo o un hurto según como se tipifique la conducta.

A continuación:

- Las aplicaciones informáticas procesan transacciones que implican movimientos de fondos (cobros, pagos o mercaderías)
- El ordenador emite documentos negociables o canjeables por dinero (cheques, pagarés, valores, etc.)

# **CAPITULO III: CLASIFICACION DE LOS DELITOS INFORMÁTICOS:**

## **1.- Delitos informáticos cometidos como fin u objetivo.**

### ***1.1- Acceso y divulgación no autorizados a servicios y sistemas informáticos.***

#### **1.1.1.- Los delincuentes informáticos**

##### **Los Hackers**

Para realizar la investigación acerca de los hackers hemos utilizado dos libros electrónicos, el primero denominado “La caza de los hackers” del autor estadounidense Bruce Sterling<sup>49</sup>, libro que puede ser copiado, de forma gratuita, para uso personal. El segundo libro de referencia se encuentra en idioma inglés y es del autor Steven Levy, denominado como “Hackers. Heroes of the Computer Revolution”<sup>50</sup>

La palabra hacker proviene del idioma inglés, y quiere decir alguien que corta troncos con un hacha, y es el término que se utilizaba para describir la manera en que los técnicos telefónicos arreglaban las cajas telefónicas descompuestas. Se denomina hacking en el argot informático a la conducta de entrar a un sistema de información sin autorización, es decir violando las barreras de protección establecidas a tal fin. El sujeto que realiza esta actividad es llamado hacker.

La actividad de hackear un sistema puede tener diferentes finalidades y alcances, se puede eliminar los pasos de seguridad de un sistema con el objeto de espiar el contenido y la información protegida, en otras ocasiones se extraen copias de la información almacenada, cambiar o destruir los contenidos de información.

Lo que caracteriza a estos sujetos es el ingreso ilegal a los sistemas informáticos, entendiendo el concepto de ingreso ilegal como la entrada de toda persona que no tiene las claves autorizadas de acceso o no las ha conseguido por los caminos lícitos.

Según los hackers<sup>51</sup> ellos desean una información libre y para ello traspasan los sistemas de seguridad de cualquier sitio electrónico que sea reconocido, aunque entre sus objetivos, según sus declaraciones, no se encuentra provocar daños o obtener beneficios de sus actividades.

<sup>49</sup> STERLING, Bruce., “La caza de los hackers” en <http://www.elaleph.com/>

<sup>50</sup> LEVY, Steven., “Hackers. Heroes of the Computer Revolution” en <ftp://metalab.unc.edu/pub/docs/books/gutenberg/etext96/hckrs10.txt>

<sup>51</sup> La página electrónica de un hacker condenado en los Estados Unidos de América, Kevin Mitnick puede revisarse en: <http://www.kevinmitnick.com/home.html>

Los hackers pueden ocasionar el colapso de las centrales telefónicas de la Policía Nacional, del número 911, del Cuerpo de Bomberos o de algún hospital, de esa forma y de manera indirecta pueden ocasionar que varias personas necesitadas de los servicios de emergencias puedan inclusive morir.

Los hackers y los preakers engañan a la gente por teléfono siempre que tienen la oportunidad de hacerlo, a este tipo de actitudes se les conoce como ingeniería social. La ingeniería social es una práctica muy común y tiene mucha efectividad. Los seres humanos son casi siempre el eslabón más débil de la seguridad informática.

Los escáneres han sido las herramientas más efectivas del hacker, se dice que un escáner que vigile a un único puerto TCP/IP tiene más eficacia que miles de claves de acceso.

Un escáner es un sistema que encuentra automáticamente los fallos de seguridad de un sistema remoto, es decir, una persona desde su habitación puede conocer los agujeros de seguridad de un sistema en otro país. Los escáneres son programas que atacan puertos TCP/IP, almacenando la respuesta que se obtiene, y así una persona puede obtener todo tipo de información de otro sistema.

Otra de las técnicas utilizadas es el cazador de contraseñas, que es un programa que descifra las contraseñas o elimina su protección. El funcionamiento es el siguiente: tomamos una palabra de una lista, la encriptamos con el protocolo que han sido encriptadas las claves, y el programa compara las claves encriptadas con la palabra encriptada que le hemos dado, si no coincide pasa a otra clave encriptada, si coincide la palabra en texto legible se almacena en un registro para su posterior visualización. Los cazadores de contraseñas que podemos encontrar son: Crack, CrackerJack, PaceCrak95, Qcrack, Pcrack, Hades, Star Cracker, etc. Hay cazadores de contraseñas para todos los sistemas operativos.

Los hackers son también una amenaza común. Se introducen a las redes simplemente por sentir emoción en el desafío o para jactarse de ello en la comunidad virtual que mantienen los hackers en el Internet.<sup>52</sup>

Los grupos de hackers se han formado con el propósito de intercambiar información relevante sobre sus actividades criminales, estos grupos se comunican a través de páginas electrónicas en la red Internet. Estos grupos nacen, florecen, declinan, comparten miembros y mantienen una gran cantidad de adeptos y aficionados.<sup>53</sup>

En el libro de Bruce Sterling, se hace referencia al ataque producido por hackers a varias centrales telefónicas de la compañía ATT, situadas en Washington DC, Pittsburgh, Los Angeles y San Francisco en los Estados Unidos de América, ataque perpetrado el 2 de julio de 1991, afectó a más de doce millones de personas y paralizó el tráfico aéreo de Nueva York lo que provocó la cancelación de 500 vuelos y otros 450 fueron retrasados, afectando aproximadamente a 85.000 pasajeros.

A raíz del ataque de hackers perpetrado a las centrales telefónicas, el Director Adjunto del Servicio Secreto de los Estados Unidos de América, Señor Garry M. Jenkis<sup>54</sup> afirmó "...nuestra experiencia demuestra que muchos sospechosos de ser hackers informáticos ya no son adolescentes descarriados, jugando maliciosamente con sus ordenadores en sus dormitorios. Algunos de ellos son operadores de ordenadores de alta tecnología y usan los ordenadores para llevar a cabo prácticas ilegales"

Los hackers generalmente no son encausados hasta que se evalúa la evidencia que se encuentra en sus ordenadores incautados, en un proceso judicial que puede tardar semanas, meses, hasta años.

Los expertos en delitos informáticos siempre han creído que las infracciones informáticas son sistemáticamente no denunciadas, algunas de las víctimas no se presentan porque creen que la

---

<sup>52</sup> Véase los siguientes sitios de hackers en el Internet: <http://www.jjf.org/>  
<http://www.geocities.com/axphackers/>

<sup>53</sup> En el libro de Bruce Sterling se mencionan varias decenas de grupos de hackers.

<sup>54</sup> STERLING, Bruce., Ob.Cit. pág. 62.

policía y los jueces no saben de informática y no pueden ni van a hacer nada. A otras empresas les avergüenza su vulnerabilidad y se esfuerzan mucho por evitar toda publicidad; por ejemplo las entidades del sistema financiero, especialmente bancos, temen la pérdida de confianza de sus clientes si se da publicidad a un caso de fraude o sabotaje informático.

Se encuentra una subdivisión de los hackers, llamados en la doctrina estadounidense como los VIRUCKERS, quienes ingresan a un sistema informático ajeno, con el objetivo de introducir un virus informático con la finalidad de destruir, alterar y/o inutilizar la información contenida en los ordenadores o sistemas informáticos.

### **Los Crackers<sup>55</sup>.**

La conducta delictiva de los Cracker se evidencia en los siguientes aspectos:

- Se introduce mediante un ordenador a un sistema informático y roba información o produce destrozos en el mismo.
- Se dedica a desproteger todo tipo de programas, tanto de versiones shareware<sup>56</sup> para hacerlas plenamente operativas y de acceso público como de programas completos comerciales que presentan protecciones que no permiten la copia.

### **Los Phreakers**

Se denomina a los Phreakers como crackers especialistas en telefonía. Sobre todo emplean sus conocimientos para poder utilizar las telecomunicaciones de forma gratuita.

Los phreakers utilizan sobre todo los denominados bridges (puentes), conferencias telefónicas ilegales de dos o más personas que utilizan las líneas telefónicas por muchas horas a cuenta de otra persona o de la compañía telefónica proveedora del servicio.

Para explicar cual es el comportamiento de este tipo de delincuentes nos referiremos a los reportes que el Director del FBI estadounidense realizó ante el Comité de Delitos Informáticos del Senado de los Estados Unidos de América<sup>57</sup>.

En septiembre de 1999, dos miembros del grupo auto - denominado como " Phonemasters " fueron condenados después de ser juzgados por hurto y posesión de los dispositivos de acceso no autorizados (§ 1029 de 18 USC) y del acceso desautorizado a un ordenador federal (§ 1030 de 18 USC). Todas estas normas constan en el Código Criminal de los Estados Unidos de América.

Los " Phonemasters " fue un grupo internacional de criminales que penetraron los sistemas informáticos de las empresas telefónicas MCI, Sprint, AT&T, y Equifax.

Con órdenes judiciales, la división de FBI en Dallas, Estados Unidos de América hizo uso nueva tecnología de la interceptación de los datos para vigilar las llamadas y los pulsos del módem de uno de los sospechosos, Calvin Cantrell. Este delincuente, Señor Cantrell, descargó millares de números de tarjetas prepago telefónico internacional de la empresa Sprint. Luego vendió esa información a un ciudadano canadiense, que luego las trasmirió a una persona residente en Ohio- Estados Unidos de América. Estos números se enviaron a un individuo en Suiza y terminaron en las manos de grupos del crimen organizado (mafia) en Italia. El señor Cantrell fue condenado a dos años de prisión.

Los métodos de este grupo criminal "Phonemasters" incluyeron la recolección de guías telefónicas antiguas y de manuales técnicos de sistemas telefónicos. Utilizaron esta información para engañar a los empleados de las empresas telefónicas a los que se les daba un falso dato

---

<sup>55</sup> Se hace referencia con este término a las personas que de manera ilegal ingresan a los sistemas informáticos y tratan de destruir o robar la información en él contenida.

<sup>56</sup> Se define al shareware como la versión de un programa de ordenador que deja al usuario utilizar ciertos componentes del programa principal, a manera de prueba del producto.

<sup>57</sup> Los reportes del Director del FBI estadounidense se pueden encontrar en: <http://www.fbi.gov>. La traducción es nuestra.

acerca de una conexión y de una falsa clave de ingreso. De allí convencían a los empleados de las empresas defraudadas que les dieran las claves verdaderas.

Es importante anotar que los delitos informáticos son facilitados a menudo por la muy conocida forma de convencer a empleados utilizando formas muy refinadas de trato con la finalidad de facilitar el que se cometan los delitos.

## ***1.2.- Daños o modificaciones de programas o datos computalizados.***

---

### **1.2.1.- Virus informáticos.-**

---

En este numeral nos guiaremos de las investigaciones que realizan las empresas proveedoras de programas antivirus tales como Symantec, Mc Afee, Inoculate IT y de la empresa Next Vision.

Un virus es un programa – una porción de código ejecutable – que tiene la habilidad única de reproducirse. Como los virus biológicos, los virus informáticos pueden diseminarse rápidamente y algunas veces son difíciles de erradicar. Se pueden adherir a cualquier tipo de archivo, se esparcen con los archivos que se copian y envían de persona a persona.

Además de reproducirse, algunos virus informáticos tienen algo en común: una rutina dañina, que el virus descarga como una bomba. Mientras que las descargas pueden ser simples mensajes o imágenes, éstas también pueden borrar archivos, reformatar el disco rígido o causar otro tipo de daño. Si el virus no contiene una rutina dañina, aún puede causar problemas, como tomar espacio libre del disco y de la memoria, y también bajar el rendimiento del ordenador.

Hace varios años la mayoría de los virus se diseminaban por medio de los discos flexibles denominados disquetes, pero el auge de Internet introdujo un nuevo mecanismo de distribución del virus. Con el correo electrónico, utilizado como la herramienta más importante de comunicación, los virus se están dispersando rápidamente. Los virus en los correos electrónicos pueden infectar toda una empresa en cuestión de minutos, con un costo de millones de dólares anualmente en productividad perdida y gastos de limpieza.

Los virus no desaparecerán en ningún momento. Más de 10,000 han sido identificados y se crean mensualmente 200 virus nuevos, de acuerdo con la International Computer Security Association. Con cifras tan alarmantes, la mayoría de las empresas luchan regularmente con ataques de virus. Nadie que use ordenadores, teléfonos celulares, computadoras Palm está inmune a un ataque con virus informáticos.

En el mes de mayo del año 2000, se detectó el virus informático que mayores pérdidas económicas ha causado hasta el momento. Se trató del VIRUS DEL AMOR, desarrollado por un joven filipino llamado Onel de Guzmán de 24 años de edad. El virus informático desarrollado afectó a millones de ordenadores en todo el mundo ya que su velocidad de propagación fue asombrosa, en dos horas se extendió desde las Filipinas hasta Alemania.<sup>58</sup>

Es necesario señalar que las pérdidas económicas que produjo el virus del amor se calcularon en diez mil millones de dólares.<sup>59</sup> Sin embargo el creador del Virus, Onel de Guzmán, no pudo ser encausado, ni menos aún juzgado ya que en las Filipinas no existía en ese momento una ley penal que castigara este tipo de ilícitos.

El Comité de Informática de la UNESCO hizo público, en ocasión de la XIV Conferencia de Autoridades Iberoamericanas de Informática, celebrada en La Habana del 13 al 18 de noviembre de 1995, un llamamiento acerca de los virus informáticos, en el que se exhortó a los gobiernos a tomar las medidas legales para que la creación y la distribución de virus informáticos fueran

---

<sup>58</sup> Ver en la Revista TIME, publicada por el diario El Comercio de Quito-Ecuador, “El Virus del Amor”, del día jueves 11 de mayo del 2.000, págs.6-10.

<sup>59</sup> The New York Times on The Web, Octubre 21 del 2.000 en <http://www.nytimes.com>

consideradas delitos y sean estas conductas penadas por la ley; asimismo, se acordó que la ONU propusiera la implementación de una solución legal a este problema.

Para la Licenciada Mariana Gómez Pérez, “el tratamiento legal de este asunto con un enfoque internacional es un imperativo de nuestro tiempo, dadas las condiciones actuales del desarrollo de la informática y la existencia de redes de información de alcance global, pero no parece tener solución práctica, al menos por el momento. Significativo, sin embargo, resulta el caso de Inglaterra, que ha establecido sanciones para los creadores y distribuidores de virus, de hasta cinco años de privación de libertad.”<sup>60</sup>

La programación de los virus informáticos ha alcanzado un nivel profesional y su accionar produce pérdidas calculadas en miles de millones de dólares, para escribir un virus ya no es necesario ser un experto en informática ni en las Nuevas Tecnologías de la Información.

### **1.2.2.- Caballos de Troya.-**

---

Este tipo de acceso no autorizado a los sistemas informáticos lleva su nombre en alusión al relato épico de Homero en la Ilíada durante la toma de Troya. Ulises mando construir un caballo de madera vacío por dentro ocultando allí gran cantidad de soldados, caballo que fue dejado en las puertas de Troya. Los troyanos pensaron que se trataba de un regalo y lo llevaron dentro de la ciudad. Allí, y en el momento menos pensado, los soldados de Ulises bajaron del caballo de madera y se tomaron la ciudad.

Se define a esta conducta atípica como la inclusión de instrucciones dentro de un programa que se utiliza de forma habitual para que realice un conjunto de funciones no autorizadas en un principio, y de esa forma, el referido programa, ejecute funciones en forma distinta a como se había previsto. Las órdenes fraudulentas se introducen, a veces con la indicación de que se auto destruyan una vez cumplida la tarea, con lo que no queda prueba del delito dentro del sistema<sup>61</sup>. De esta forma bajo la apariencia inofensiva del programa y sin conocimiento del sujeto víctima del ilícito, desencadena una serie de daños y estragos.

Un ejemplo de esta conducta la describe el profesor chileno Jijena Leiva<sup>62</sup> y se manifiesta en el introducir una modificación al programa del tratamiento de cuentas corrientes y se consulte un saldo, el programa caballo de troya envía la información del saldo de la cuenta y luego multiplica el saldo por dos, tres, cuatro, cien, mil, etc. con lo que es posible autorizar pagos o transferencias que no tengan sustento en los fondos reales del cuenta correntista.

### **1.2.3.- Puertas Falsas.-**

---

En el desarrollo de aplicaciones complejas, es habitual que los programas permitan introducir interrupciones en la lógica de los mismos, con el objeto de revisar por medio de procesos informáticos, si los resultados intermedios son correctos, producir salidas de emergencia y de control a fin de salvaguardar resultados parciales para luego comprobarlos. Inclusive algunas veces este procedimiento se enlaza con rutinas del sistema operativo para facilitar una "puerta de entrada al programa" que no estaba prevista, pero de esta manera facilitan la labor de desarrollo y prueba del programa.

Para evitar este tipo de delitos, todas las puertas falsas deben desaparecer cuando los programas entran en proceso de producción normal.

---

<sup>60</sup> GÓMEZ PEREZ, Mariana., “Los Virus informáticos: Criminalidad informática: un fenómeno de fin de siglo. En [http://publicaciones.derecho.org/cubalex/N%BA\\_07\\_Ener-Mar\\_1999/2](http://publicaciones.derecho.org/cubalex/N%BA_07_Ener-Mar_1999/2) Revista Electrónica de Estudios Jurídicos (CubaLex) (Cuba)

<sup>61</sup> GUIBOURG y otros., Ob.Cit. pág.225.

<sup>62</sup> JIJENA LEIVA, Renato Javier, “ Chile, La protección penal de la intimidad y el delito informático” Editorial Jurídica de Chile, pág.95.

Muchos fabricantes de software dejan puertas falsas no eliminadas, puertas que por ser temporales no constan en la documentación del sistema, y de esa manera permiten el ingreso no autorizado a programas de ordenador o bases de datos.

El caso Rifkin<sup>63</sup> describe claramente dos conductas atípicas y delincuenciales, la empresa perjudicada fue un banco de la localidad de Los Angeles, California, Estados Unidos de América, que registraba un movimiento diario de decenas de millones de dólares al día en transferencias electrónicas de fondos. Santaley Rifkin, un técnico informático, fue contratado por el banco para preparar una copia de respaldo del programa empleado para concretar las transferencias. Rifkin descubrió en el sistema algunas puertas falsas que permitían hacer transferencias ilegales. Finalizada su tarea, retuvo una tarjeta plastificada que le permitía a la sala de transferencias. Luego de haber concluido el trabajo para el que fue contratado, ingresó a la sala antes referida y manifestó a los empleados bancarios presentes, con los que tenía ya un trato amistoso, que debía verificar el funcionamiento del sistema y comprobó que éste era exactamente el que el había instalado. Tomó nota del código vigente en el momento, que se cambiaba varias veces al día, y salió del banco. Inmediatamente se conectó con el sistema del banco usando para este fin un pequeño computador y logró transferir a su cuenta bancaria en Nueva York diez millones doscientos mil dólares, que luego trasladó a un banco suizo. A su vuelta de Europa fue descubierto, procesado, condenado y encarcelado. El caso de Rifkin fue el primer caso célebre de un delito informático.

#### **1.2.4.- Bombas lógicas. –**

---

Este tipo de conductas atípicas se definen como las actividades destructivas de programas que comienza tras un plazo, sea por el transcurso del tiempo, por ejemplo a los tres meses o en una fecha o a una hora determinada, o por la presencia de un dato, de un código, o cualquier mandato que, de acuerdo a lo determinado por el programador, es identificado por el programa como la señal para empezar a actuar.

La jurisprudencia francesa registra un ejemplo de este tipo de casos. Un empleado programó el sistema de tal forma que los ficheros de la empresa se destruirían automáticamente si su nombre era borrado del rol de pagos.

Las bombas lógicas también pueden ser distribuidas por medio del correo electrónico, las que se las denomina bombas de correo electrónico. Estas bombas tienen la capacidad para crear grandes cantidades de tráfico de correo electrónico “E-mail (electronic mail)” apuntadas a uno o varios servidores. Si el servidor no tiene la capacidad de manejar la cantidad masiva de tráfico del correo electrónico, puede colapsar requiriendo el reinicio del sistema o la otra medida correctiva.

En la economía globalizada actual, el comercio electrónico desempeña un punto muy importante, más este tipo de bombas son extremadamente perjudiciales para una compañía que fundamenta su negocio en el comercio electrónico y en los sitios en el Internet.

Existen otro tipo de bombas de correo electrónico en las cuales los delincuentes informáticos usan logotipos falsos de compañías u organismos de gobierno para desacreditar organizaciones y para afectar la disponibilidad de los sistemas de comunicaciones por vía del correo electrónico.

El delincuente informático puede ejecutar un programa para enviar múltiples correos electrónicos y quizás continuos, a una cadena de los servidores. Si el primer servidor en el cadena acepta la bomba de correo electrónico, pasará el correo electrónico al segundo servidor y así de forma sucesiva. Esta operación puede producir la negación o desaceleración del servicio de correo electrónico del servidor que se ha fijado como objetivo.

---

<sup>63</sup> MASSA, Lilli., “Delitos informáticos” trabajo presentado en las I Jornadas de Informática al servicio del Derecho, Mercedes, 1985. Citado por GUIBOURG y otros, Ob.Cit., pág.276.

Es muy importante que las entidades públicas y privadas del Ecuador tomen muy en cuenta este tipo de ilícitos con la finalidad de evitar colapsos en sus servidores informáticos. Una interferencia o daño en estos sistemas son cuantificados en pérdidas de millones de dólares al año.<sup>64</sup>

### **1.2.5.- Gusanos Informáticos.-**

---

Se crean de manera muy similar a los virus informáticos, y se utilizan con la finalidad de infiltrarlo en programas de procesamientos de datos para alterar, modificar o destruir los datos. El virus informático se reproduce en un ordenador que sirve de portador y el gusano informático se reproduce a lo largo de toda la red informática<sup>65</sup>.

Las consecuencias de un ataque a un sistema informático con este tipo de programas puede ser tan grave como un ataque con virus informáticos.

Existen además otras técnicas que se ajustan a esquema del ilícito informático, entre las que podemos señalar:

- Modificación de documentos fuentes, que se refiere a la información destinada a ser procesada o “data diiddling” (datos engañosos, por su traducción al castellano) Es una de las conductas más elementales pero una de las más seguras y eficaces, por cuanto las manipulaciones hechas antes o durante la entrada de los datos al ordenador son difíciles de detectar.
- Técnicas del salame o redondeo para abajo.- Método utilizado de manera general en Instituciones del Sistema Financiero donde se producen transferencias electrónicas de dinero y que consiste en la sustracción de pequeñas cantidades de activos de distintas procedencias haciendo un redondeo de las respectivas cuentas y depositando el remanente producido en otra cuenta de libre disposición.
- Superzapping.- “Es el uso no autorizado de un programa de utilidad para alterar, borrar, copiar, insertar, o utilizar en cualquier forma no permitida datos almacenados en el ordenador o en soportes magnéticos.”<sup>66</sup>
- Recogida de información residual.- “ Este procedimiento se basa en aprovechar los descuidos de los usuarios o los técnicos informáticos para obtener la información que ha sido abandonada sin ninguna protección como residuo de un trabajo real efectuado con autorización.”<sup>67</sup>

### **1.3.- Fraude informático.-**

---

Según Carlos Romeo Casabona, el fraude informático es “ la incorrecta utilización del resultado de un procesamiento automatizado de datos, mediante la alteración en cualquiera de las fases de su procesamiento o tratamiento informático, siempre que sea con ánimo de lucro y en perjuicio de tercero. Por ejemplo, al ingresar datos falsos, manipular programas computacionales con fines ilícitos, o al alterar los datos procesados que salen por los dispositivos periféricos”.<sup>68</sup>

---

<sup>64</sup> La bombas de correo electrónico han sido catalogadas por el FBI de los Estados Unidos de América como atentatorias a la seguridad nacional. Véase los informes del Director del FBI al Senado de los Estados Unidos en : <http://www.fbi.gov.statment>

<sup>65</sup> El virus del amor, descrito anteriormente es clasificado también como gusano informático.

<sup>66</sup> CAMACHO Losa, Luis, “El Delito Informático” p. 42. Citado por MAGLIONA, Claudio y LÓPEZ , Macarena., Ob.Cit.pág.47.

<sup>67</sup> Ibídem., pág.47.

<sup>68</sup> ROMEO CASABONA, Carlos., “ Poder informático y Seguridad Jurídica” Fundesco, Madrid, España, 1987.

Los distintos métodos para realizar estas conductas se deducen, fácilmente, de la forma de trabajo de un sistema informático: en primer lugar, es posible alterar datos, omitir datos verdaderos o introducir datos falsos, en un ordenador.

Ulrich Sieber, cita como ejemplo de esta modalidad el siguiente caso tomado de la jurisprudencia alemana:

Una empleada de un banco del sur de Alemania transfirió, en febrero de 1983, un millón trescientos mil marcos alemanes a la cuenta de una amiga - cómplice en la maniobra- mediante el simple mecanismo de imputar el crédito en una terminal de computadora del banco. La operación fue realizada a primera hora de la mañana y su falsedad podría haber sido detectada por el sistema de seguridad del banco al mediodía. Sin embargo, la rápida transmisión del crédito a través de sistemas informáticos conectados en línea (on line), hizo posible que la amiga de la empleada retirara, en otra sucursal del banco, un millón doscientos ochenta mil marcos unos minutos después de realizada la operación informática<sup>69</sup>

Los objetos sobre los que recae la acción del fraude informático son generalmente los datos informáticos relativos a activos o valores que en la mayoría de los casos estos datos representan valores intangibles (ejemplo: depósitos monetarios, créditos, etc.), en otros casos, los datos que son objeto del fraude, representan objetos corporales (mercadería, dinero en efectivo, etc.) que obtiene el autor mediante la manipulación del sistema.

En las manipulaciones referidas a datos que representan objetos corporales, las pérdidas para la víctima son, generalmente, menores ya que están limitadas por la cantidad de objetos disponibles. En cambio, en la manipulación de datos referida a bienes intangibles, el monto del perjuicio no se limita a la cantidad existente sino que, por el contrario, puede ser creado por el autor.

Como se puede apreciar, las conductas descritas afectan la propiedad. Un punto interesante es analizar si la legislación penal vigente en nuestro país comprende, en sus disposiciones legales, estas nuevas modalidades delictivas que afectan al patrimonio. El problema fue objeto de un profundo análisis doctrinario y jurisprudencial en el derecho comparado, generando incluso la preocupación de organismos internacionales que dedicaron convenciones especiales al estudio del tema y formularon recomendaciones que dieron lugar a la modificación de la legislación penal en algunos países.

En la República Federal de Alemania las lagunas legales que este tipo de casos dejaban en evidencia, especialmente por la necesidad típica en la figura del fraude informático, determinó la introducción de un agregado al tipo penal del fraude (parágrafo 263 a del StGB), en el que se establece:

“El que, con la intención de procurarse a sí mismo o a un tercero un beneficio patrimonial antijurídico, causare un perjuicio en el patrimonio de otro, determinando el resultado de una operación de proceso de datos mediante la incorrecta configuración del programa, el empleo de datos incorrectos o incompletos, el empleo no autorizado de datos o cualquiera otra intervención ilegítima en el curso del proceso, será sancionado con pena de prisión de hasta cinco años o pena de multa.”

Parte de la doctrina sostiene que, en los casos en que el autor manipula el sistema causando un perjuicio pero sin inducir a error a una persona, su conducta no sería típica de los delitos de defraudación.

Observemos el siguiente caso de la legislación argentina: El autor del delito, empleado del Citibank, tenía acceso a las terminales de computación de la institución bancaria. Aprovechando esta circunstancia utilizó, en varias oportunidades, las terminales de los cajeros, cuando ellos se retiraban, para transferir, a través del sistema informático, fondos de distintas cuentas a su cuenta personal. Posteriormente, retiró el dinero en otra de las sucursales del banco.

---

<sup>69</sup> SIEBER, Ulrich., Handbook Crime Computer, pág. 6.

En primera instancia el Juez calificó los hechos como constitutivos del delito de hurto en forma reiterada.

La Cámara del crimen de la República Argentina resolvió:

“... y contestando a la teoría fiscal, entiendo que le asiste razón al Dr. Galli en cuanto sostiene que estamos en presencia del tipo penal de hurto (art. 162 del Código Penal) y no de estafa (art. 172). Ello es así porque el apoderamiento lo hace el procesado y no le entrega el banco por medio de un error, requisito indispensable para poder hablar de estafa. No veo en los presentes la ecuación del delito de estafa: ardid - error - disposición patrimonial voluntaria, sino que, tal como aparece en autos y ha sido narrado, el apoderamiento lo hace el procesado directamente, manejando el sistema de computación. De manera que no hay diferencia con la maniobra normal del cajero, que en un descuido se apodera del dinero que maneja en caja y la maniobra en estudio en donde el apoderamiento del dinero se hace mediante el manejo de la computadora...”<sup>70</sup>

Otro caso descrito por el Director del FBI estadounidense, es el siguiente: Dos jóvenes de 18 años fueron arrestados en Gran Bretaña y acusados de vulnerar sitios de comercio electrónico de cinco países por la Internet, sustraer información sobre más de 26.000 tarjetas de crédito y divulgar parte de esta información en el Internet. Los jóvenes fueron arrestados con relación a la incursión furtiva de los sitios de Internet de nueve empresas de Estados Unidos, Canadá, Tailandia, Japón y el Reino Unido durante los últimos meses. Los sospechosos, cuyos nombres las leyes británicas prohíben divulgar, fueron arrestados en sus hogares, por el Servicio de Policía de Dyfed-Powys. Las incursiones furtivas, fueron perpetradas bajo el nombre de "Curador" y pueden haber causado pérdidas superiores a los 3 millones de dólares. Dicha cantidad cubriría el costo promedio a la industria de las tarjetas de crédito por cerrar más de 26.000 cuentas y expedir tarjetas nuevas, aunque se estima que habría otros costos, incluso la reparación de los sitios informáticos y cualquier pérdida padecida por los clientes cuyos números de tarjeta de crédito hayan sido usados ilícitamente. Los proveedores de servicios de Internet cerraron esos sitios en varias ocasiones, pero "Curador" resurgía en otros lugares del Internet en cuestión de horas.<sup>71</sup>

Revisemos ahora otro caso: L. Levin y sus cómplices transfirieron de manera ilegal más de \$10 millones de dólares a partir de tres clientes corporativos de Citibank y las enviaron a cuentas bancarias en California, Finlandia, Alemania, los Países Bajos, Suiza, e Israel entre junio y octubre de 1994. Levin, especialista en computadoras ruso, accedió mas de cuarenta veces al sistema informático de la tesorería de Citibank usando un ordenador personal, con claves y números de identificación robados. Los empleados rusos de la compañía del teléfono que trabajaban con Citibank pudieron rastrear la fuente de las transferencias y dieron con un teléfono de Levin en San Petersburgo, Rusia. Levin fue arrestado en marzo de 1995 en Londres y fue extraditado posteriormente a los Estados Unidos de América, el 24 de febrero del 1998; un juez condenó a Levin a tres años en la prisión y fue ordenado pagar al Citibank \$240.000 como restitución. Citibank solo pudo recuperar \$400.000 de los fondos ilegalmente transferidos.<sup>72</sup>

#### **1.4.- Transferencia de fondos.**

---

La criminalidad organizada aprovecha de los medios informáticos, telemáticos y satelitales de diferente forma para cometer, u ocultar la comisión de delitos.<sup>73</sup>

#### **1.5.- Sabotaje informático**

---

Con la finalidad de explicar de mejor forma el delito informático que se ha denominado sabotaje informático, seguiremos la opinión de varios tratadistas chilenos<sup>74</sup> sobre este tema, ya que en ese

---

<sup>70</sup> Fallo judicial argentino citado por Huerta Miranda, Marcelo., “Figuras Delictivo - Informáticas Tipificadas En Chile. Desarrollo Y Análisis De Las Figuras Delictivo Informáticas Tipificadas En La Ley” en <http://derecho.org>

<sup>71</sup> Reporte del Director del FBI ante el Senado Estadounidense en <http://www.fbi.gov>.

<sup>72</sup> Ibídem.

<sup>73</sup> Sobre las transferencias de fondos se amplía en el numeral en donde se trata sobre el delito de narcotráfico.

país ha sido promulgado una ley penal que tipifica los delitos informáticos desde el 7 de junio de 1993.

Se define al sabotaje informático como “ la destrucción o inutilización del soporte lógico, esto es, de datos y/o programas contenidos en un ordenador (en sus bandas magnéticas) El término sabotaje informático comprende todas aquellas conductas dirigidas a causar daños en el hardware o en el software de un sistema informático, o telemático.”<sup>75</sup>

Para el doctor Marcelo Huerta Miranda, el sabotaje informático es “ toda conducta atípica, antijurídica y culpable que atente contra la integridad de un sistema de tratamiento de información o sus partes componentes, su funcionamiento o los datos contenidos en él.”<sup>76</sup>

El causante del sabotaje informático puede ser un agente externo a la empresa o por el contrario, un agente interno, esto es, los propios empleados. Hay varios estudios que ponen de relieve los daños que se realizan por medios informáticos. Si algo hay que destacar en primer lugar es la desproporción entre el gran perjuicio que se puede causar y la gravedad del ataque, así como la dificultad de valorar este daño.

### ***Clases o tipos de sabotaje informático:***

---

#### **Acciones contra el sistema de tratamiento de la información.**

---

Esta categoría comprende tanto la destrucción o inutilización de un sistema automatizado de tratamiento de la información, respecto de la totalidad de este, como asimismo, en cuanto a sus partes componentes.

Los acciones de destruir e inutilizar el sistema de tratamiento de la información, constituyen un atentado de tipo directo, por cuanto importan un daño de tipo permanente o irreversible.

**a.1. Respecto de la totalidad del sistema de tratamiento de la información.** La conducta punible apunta a deshacer o quitar forma a un sistema de tratamiento de la información sea en su elemento lógico (software) y material (hardware).

Respecto del elemento lógico (software) este, por su naturaleza jurídica, escapa a la esfera de protección penal común, precisando una tutela especial cuando las acciones punibles son realizadas mediante la ejecución de medios de tecnología computacional, con resultado típico destrucción o inutilización.

El elemento material por su parte (hardware), su naturaleza de bien corporal mueble implica que al consumarse su verbo rector en el tipo, deba ser sancionado por la figura del delito de daños en el Código Penal Ecuatoriano.

a.2. Respecto a las partes componentes del sistema de tratamiento de la información.

b. Acciones contra el funcionamiento de un sistema de tratamiento de la información. Estas, a su vez, admiten la siguiente subclasificación:

b.1.- Impedir el funcionamiento del sistema.- Impedir según el diccionario de la Real Academia Española de la Lengua (RAE), significa: "estorbar, imposibilitar la ejecución de una cosa". Del latín "impedire", implica que no puede usar de sus miembros ni manejarse para andar.

---

<sup>74</sup> HUERTA MIRANDA, Marcelo., “Figuras Delictivo - Informáticos Tipificadas En Chile. Desarrollo Y Análisis De Las Figuras Delictivo Informáticas Tipificadas En La Ley” en <http://derecho.org>, JIJENA LEIVA, Renato Javier. Ob.Cit. pág.95. MAGLIONA, Claudio., y LÓPEZ, Macarena, Ob. Cit.54

<sup>75</sup> ROMEO CASABONA, Carlos María, “ Poder informático y Seguridad Jurídica, Fundesco, Madrid, España, 1987. Citado por MAGLIONA , Claudio y LÓPEZ M. Macarena., Ob.Cit. pág.56

<sup>76</sup> . HUERTA MIRANDA, Marcelo. Ob.Cit

b.2.- Obstaculizar el funcionamiento del sistema de tratamiento de la información.- Para el diccionario de la RAE , la palabra obstaculizar significa:  
" Impedir o dificultar la consecución de un propósito".

En cuanto a su acepción y repercusión esta dificultad se traduce en un entorpecimiento en el funcionamiento de un sistema, sin perjudicar la existencia del mismo.

**b.3.- Modificar el sistema de tratamiento de la información o de sus partes componentes.** De acuerdo a su definición, esta palabra cuya raíz latina *modificare*, en su acepción filosófica significa: "Dar un nuevo modo de existir a la substancia material".(De acuerdo al diccionario de la RAE).

La cosa, en este caso el sistema de tratamiento de la información, debe entenderse mutada en razón del objeto o función para la que fue concebida, es decir en razón de su eficiencia.

Un sistema de tratamiento de información " está concebido y orientado por su naturaleza a satisfacer determinados requerimientos específicos de un determinado usuario por medio de las ciencias informáticas, y para el cual es diseñado, motivo por el cual su funcionamiento debe ser idóneo. De manera que se varía su forma de servir se desviará de su objeto específico. Lo anterior nos lleva a reflexionar sobre el aspecto probatorio de este tipo de atentado, para lo cual pensamos que el juez deberá no sólo apoyarse en la comparación del funcionamiento actual del sistema en relación con su funcionamiento original, sino que además buscar auxilio en las especificaciones de requerimientos u otros documentos que lo ilustren sobre sus características y funcionamiento."<sup>77</sup>

### **c. Conductas que afectan los datos contenidos en un sistema de tratamiento de la información.**

**1. La alteración de datos.-** Alterar según el diccionario de la RAE significa: "Cambiar la esencia o forma de una cosa". La voz *alterar*, es omni comprensiva de conductas como el ingreso de datos erróneos, el borrado de datos verdaderos, de transformaciones y desfiguraciones de los datos, y en general, de toda conducta que implique el cambiar la información contenida en un sistema de tratamiento de la misma sin destruirla.

Estas conductas, están recepcionadas, aunque con distintas denominaciones y sistematizadas en el derecho comparado.<sup>78</sup>

**2. Dañar o destruir los datos.-** Dañar, significa "Maltratar o echar a perder una cosa". (Diccionario de la RAE). En relación con los datos contenidos en un sistema de tratamiento de la información esta se entiende como una conducta destinada a perjudicar la integridad de la información, lo que plantea la noción de un perjuicio, maltrato o afectación de una cosa.

Perjudicada la integridad de un sistema de tratamiento de la información, se afectará el fin u orientación específica del mismo, lo que en el caso de dañarse implica una conducta de carácter transitorio y reversible.

Destruir, de acuerdo a la RAE implica, "Deshacer, arruinar o asolar una cosa...". En razón de su significado implica un concepto amplio, permanente e irreversible, cuya entidad se traduce en la pérdida de los datos a través de su desfiguración.

El elemento constitutivo del delito informático aparece constituido, en el caso del sabotaje informático, por el dolo que en el caso referido, debemos concluir que se trata del dolo directo.

---

<sup>77</sup> HUERTA MIRANDA, Marcelo. Ob.Cit.

<sup>78</sup> El capítulo IV de esta investigación esta dedicado exclusivamente a detallar las normas penales en el derecho comparado.

## CLASIFICACIONES DEL DOLO

1.-DOLO DIRECTO <sup>79</sup> “ es la forma más característica de dolo. Se presenta cuando el sujeto activo no sólo realiza la conducta típica de modo voluntario y consciente, sino que está animado del propósito preciso de obtener la producción del hecho jurídicamente reprochable inserto en dicha conducta.

2.-DOLO DE LAS CONSECUENCIAS SEGURAS o como lo denominaba Jiménez de Asúa, dolo de las consecuencias necesarias, estimándolo una especie de dolo directo. Se presenta en el caso que entre lo previsto y lo deseado por el agente no hay una plena concordancia pero si bien parte de las consecuencias no fue querida por el actor, ella fue aceptada como imprescindible para la producción del resultado efectivamente buscado.

3.-DOLO EVENTUAL es aquella forma de dolo que surge cuando el sujeto se representa la posibilidad de un resultado que no desea pero cuya producción ratifica en último término.”

Veamos ahora el siguiente caso de sabotaje informático con la finalidad de ilustrar lo tratado.

En 1997, George Parente fue detenido por realizar un bloqueo de cinco servidores de la red en la compañía que publica Forbes Inc. Parente era un técnico de Forbes que había terminado su empleo temporal en esa empresa. Luego de dejar su empleo se conectó desde su domicilio al sistema informático de Forbes, con la ayuda de un ordenador y una clave que fue copiada de un ex compañero de trabajo. Una vez que esté conectado causo el bloqueo de cinco de los ocho servidores de la red de ordenadores de Forbes, y borró toda la información que se encontraba en cada uno de los servidores afectados. Ninguno de los datos borrados pudo ser recuperado. El sabotaje de Parente no permitió a la empresa Forbes abrir durante dos días las operaciones de Forbes en Nueva York con las pérdidas en sus operaciones en la Bolsa de Valores de Nueva York, lo que provocó un lucro cesante y daño emergente por el orden de \$100.000 dólares. Parente fue encausado y declarado culpable en base al Acta de Abuso Informático del Código 18 U.S.C. 1030 de los Estados Unidos de América.<sup>80</sup>

## 2.- Delitos informáticos cometidos como medio o instrumento para perpetrar otros delitos.

### 2.1.- Pornografía.

El Internet es uno de los espacios mas utilizados por quienes intentan colocar material de contenido sexual explícito o similar. Se estima que alrededor de un 15% de todo el material que circula en el Internet tienen un contenido pornográfico y/o intolerante.

Se coloca el material en páginas de alojamiento gratuito o pagado, puede tratarse de fotos, videos, relatos u otro tipo de imágenes digitalizadas.

En algunas de las páginas que contienen este tipo de material se toman el trabajo de crear un código de verificación de edad a través del cual se verifica que la persona que esta navegando sea mayor de 18 años. Los sistemas de verificación de edad requieren el uso de tarjetas de crédito y como no hay demasiadas personas dispuestas a otorgar su numero de tarjeta por la red Internet.

El servicio de correo electrónico (e-mail, en el idioma inglés) se ha visto afectado en forma indirecta, muchas personas que se dedican a enviar material explícito (en cualquier formato digital).

Al tratar este tema nos realizamos las siguientes preguntas: ¿Cuál es la ley aplicable para determinar si el material exhibido es o no pornográfico, presenta o no contenido discriminatorio ? ¿

<sup>79</sup> HUERTA MIRANDA, Marcelo. Ob.Cit.

<sup>80</sup> Presentación del Director del FBI. Dirección electrónica de Internet citada anteriormente.

Tal vez la ley del lugar de asiento físico del servidor, la ley del lugar en donde las páginas electrónicas se pueden acceder, la ley del lugar físico desde donde se intercambia el material?

Determinada la ley aplicable, debemos buscar a la persona que debe ser sujeta a sanción penal a quien debe sancionarse, a los que arman la página con contenido sexual, a los que la accedan, a quien provee el alojamiento o prestan su servidor de conversaciones en tiempo real y/o Chat, para intercambiar material.

Existen en la jurisprudencia estadounidense fallos judiciales sobre el tema referido, como el caso de Felix Somm, conocido como caso Compuserve. La empresa Compuserve de capitales alemanes y norteamericanos brindaba desde sus servidores en Alemania acceso mundial a varios sitios de contenidos pedófilos. Procedida la denuncia en Estados Unidos de América se allanaron las sedes de la empresa en Alemania y Felix Somm fue encontrado penalmente responsable de contribuir al delito de divulgación de pornografía infantil<sup>81</sup>

Con la finalidad de tratar de solucionar este problema el gobierno australiano ha creado un organismo oficial el Australian Broadcasting Authority (ABA), que deberá regular el contenido de Internet según una ley sancionada por la legislatura australiana.

Este trabajo de investigación no pretende censurar los contenidos de Internet, sin embargo estamos plenamente convencidos que se debe evitar la difusión de material altamente ofensivo que puede afectar a niños y a adolescentes.

## **2.2.- Narcotráfico.**

Se utiliza los medios y sistemas informático para blanquear el dinero proveniente de esta actividad ilícita.

Las modalidades de blanqueo de dinero en la banca convencional y en la banca electrónica de acuerdo con los informes de el Grupo de acción Financiera (GAFI)<sup>82</sup>

1. Ingresar grandes sumas de dinero en efectivo en una cuenta, con el fin de efectuar inmediatamente una transferencia electrónica a otra cuenta.
2. Numerosos depósitos de pequeñas cantidades, situadas por debajo de la obligación de declarar y en varias cuentas, desde las que se efectúan transferencias a otra cuenta, generalmente en el extranjero.
3. Uso de entidades off shore.
4. Introducción de personas de confianza en pequeñas entidades financieras o en delegaciones.
5. Cuentas de colecta o recaudación: Un número importante de inmigrantes hacen pequeños ingresos sucesivos que envían al exterior en forma agrupada.
6. Depósitos en cuentas extranjeras de una cantidad que actúa como garantía de un préstamo que es enviada al país de origen como una operación legítima que justifica la recepción de ese capital.
7. Las transferencias electrónicas son el principal instrumento utilizado en el blanqueo de dinero, debido a la rapidez con que se transfiere de un país a otro.
8. A pesar de la mejora en los sistemas de identificación de los clientes en las entidades financieras, sigue el problema de identificar de manera plena a la persona que ordena la transferencia.

<sup>81</sup> Sobre el tema puede revisarse las siguientes direcciones electrónicas: <http://www.stop-childpornog.at/>, <http://www.info2000.csic.es/midas-net/pornoinfantil.htm>

<sup>82</sup> Los informes de GAFI sobre el blanqueo de dinero se encuentran en <http://oecd.org/fatf/index.html>.

### **2.3.- Terrorismo.**

---

El terrorismo informático se define como el uso de la tecnología informática y telemática con el objetivo de atacar infraestructuras nacionales críticas (tales como energía, transporte, u operaciones del gobierno) con el fin de intimidar a naciones enteras.

Muchos grupos terroristas del mundo están utilizando cada vez más las nuevas tecnologías informáticas y del Internet para formular planes, recaudar fondos, hacer propaganda, y comunicarse con seguridad. Grupos como la banda terrorista ETA (EUSKADI TA ASKATASUNA) e IRA (EJÉRCITO REPUBLICANO IRLANDES) incluyendo Hizbollah, HAMAS, la organización de Abu Nidal, y del terrorista Osama Bin Laden están utilizando ficheros automatizados, correo electrónico, y el cifrado de mensajes para utilizar sus operaciones.

En ocasión del levantamiento palestino de octubre y noviembre del 2.000 se ha hecho evidentes ataques perpetrados directamente por organizaciones terroristas a sitios del gobierno estadounidense e israelitas, así como empresas multinacionales de capitales de ciudadanos de las naciones referidas anteriormente. La finalidad de los ataques es tratar de inutilizar los sistemas automáticos de información, y de las sitios en el Internet, mediante el envío de virus informáticos, gusanos, bombas lógicas, de otros mecanismos considerados como conductas delictivas enmarcadas en el sabotaje informático.

### **2.4.- Espionaje.**

---

Revisemos la siguiente definición de espionaje informático: " Es toda conducta típica, antijurídica y culpable que tiene por finalidad la violación de la reserva u obligación de secreto de la información contenida en un sistema de tratamiento de la información".<sup>83</sup>

En el derecho comparado se ha entendido por espionaje informático, aquel delito que consiste en obtener una información de forma no autorizada, sea por motivo de lucro o de simple curiosidad, hecho que implica espiar y procurarse una comunicación o bien una utilización de un sistema de tratamiento de la información en forma desleal, no autorizada.

Se clasifica al delito de espionaje informático en:

- a) Delitos de apoderamiento, uso o conocimiento indebido de la información contenida en un sistema automatizado de tratamiento de la información.
- b) Delitos de revelación indebida y difusión de datos contenidos en un sistema de tratamiento de la información.

Se pensaba de forma general que la comisión de un delito informático era facultad de personas, que tenían conocimientos relacionados con la Informática y las Nuevas Tecnologías de Información. En la actualidad, existe un consenso en el derecho comparado de estimar que cualquier persona puede ejecutarlos, no es necesario que se inviertan miles de dólares para la compra de equipos sofisticados para el cometimiento del delito de espionaje informático.

En la actualidad este delito preocupa especialmente a las empresas, es aquí justamente donde ha sido evidente ya que puede ser muy lucrativo para su autor, lo que lo hace especialmente peligroso y con enormes repercusiones técnicas y económicas.

Hay un caso célebre descubierto por el Servicio de Contraespionaje de la República Federal Alemana en 1989, en el cual un grupo de jóvenes alemanes expertos en Informática, pagados por la KGB soviética accedieron a los datos de los sistemas de el Pentágono, la NASA, del Consorcio Franco-Italiano Thomson, del Centro de Investigaciones Nucleares de Ginebra, de la Agencia Espacial Europea y del Instituto Max Planck de física nuclear en Heidelberg entre otros.

---

<sup>83</sup> HUERTA MIRANDA, Marcelo. Ob.Cit.

En el campo del espionaje informático donde queda más al descubierto la precariedad de los sistemas de seguridad, incluso estatales y la vulnerabilidad de los sistemas de tratamiento de la información, de los datos en él contenidos y de la gravedad e importancia a nivel internacional del problema de la creciente criminalidad informática.

Los tratadistas chilenos<sup>84</sup> siguiendo el texto de la Ley de Delitos Informáticos Chilena vigente, clasifican de la siguiente manera al delito de espionaje informático:

**a) Delitos de apoderamiento, uso o conocimiento indebido de la información contenida en un sistema automatizado de tratamiento de la información.**

**1.- Interferencia de la información contenida en un sistema de tratamiento de la información.-** Interferir: Según el diccionario de la RAE significa, "cruzar, interponer algo en el camino de una cosa, o en una acción. Causar interferencia".

La interferencia supone una alteración de la calidad, pureza e idoneidad de la técnica de la ciencia informática, mediante la acción recíproca de las ondas de la que resulta un aumento, disminución o neutralización del movimiento ondulatorio original de los impulsos eléctricos, operada utilizando métodos tecnológicos modernos, ya sea con el fin de apoderarse de ella, de usarla o de conocerla.

**2.- Intercepción indebida de la información contenida en un sistema de tratamiento de la información.-** Interceptar según la RAE significa; "apoderarse de una cosa antes que llegue al lugar o a la persona a quien se destina". De manera que la conducta descrita supone que la información contenida y transmitida en un sistema de tratamiento de la misma no dejará por la intercepción de llegar a su destino o destinatario, pues por su naturaleza de bien incorpóral no se ve limitada por el apoderamiento, uso o conocimiento a un sólo poseedor.

**3.- Acceso indebido a la información contenida en un sistema de tratamiento de la misma.-** El acceso indebido a la información consiste en las pericias tendientes a introducirse en un sistema de tratamiento de la información, burlando todas las medidas de seguridad y resguardo programadas en su entrada, con el fin de allegarse a la información reservada contenida en el sistema, recabarla y eventualmente utilizarla en beneficio o en perjuicio de terceros.

Desde esta perspectiva, el acceso indebido implica una violación de las claves del sistema, las cuales pueden haberse producido de manera premeditada por su autor, o bien, accidentalmente, es decir, la vulneración de las medidas de seguridad no estaban en el ánimo del delincuente, sin embargo, una vez en el sistema, el agente se apodera, conoce o utiliza la información confidencial a que no tenía derecho.

## ***2.5.- Espionaje Industrial.***

---

En este numeral tomaremos muy en cuenta las opiniones del Dr. Manfred Mohrenschaeger<sup>85</sup> quien afirma que los secretos empresariales y el valioso know how son almacenados en ordenadores o computadores. Junto a las formas tradicionales de espionaje económico, han surgido un nuevo tipo de delito, el espionaje informático. De esta forma el objeto del delito puede ser tanto el hardware como el software, además de los datos almacenados, desempeñando un papel de gran importancia la copia y uso no autorizado de programas de computadora.

El delito puede ser cometido por la copia ilícita de datos almacenados y la intervención de las líneas de transmisión de datos, es decir a intervención de la transmisión o de las radiaciones electrónicas de las pantallas de los terminales.

---

<sup>84</sup> HUERTA MIRANDA, Marcelo. Ob.Cit.

<sup>85</sup> MOHRENSCHALEGER, Manfred, "Tendencias de la Política Jurídica en la Lucha contra la Delincuencia Relacionada con la Informática" exposición en el seminarios hispano - alemán celebrado en la Universidad de Barcelona, sobre la delincuencia informática, cuya recopilación fue realizada por MIR PUIG, Santiago, Citado por MAGLIONA, Claudio y LÓPEZ, Macarena. Ob.Cit. Págs. 92-93

# **CAPITULO IV: LOS DELITOS INFORMÁTICOS EN EL DERECHO COMPARADO**

## **1.Generalidades**

En este capítulo de la investigación se hará referencia a las leyes penales en materia informática de los Estados Unidos de América, de la Comunidad Económica Europea; en donde además de revisar la Legislación Comunitaria europea vigente, revisaremos la Legislación de Alemania, Francia y España, de la República de Chile, Estados Unidos Mexicanos, de la República del Perú y un proyecto de ley de delitos informáticos de la República de Colombia.

Es muy importante señalar que los esfuerzos por tipificar las conductas ilícitas que se han denominado en doctrina como delitos informáticos vienen desde la segunda mitad de la década de 1980, a pesar de ello algunos países no se han tomado la molestia de estudiar e investigar el fenómeno informático. Por ello la necesidad de recurrir al derecho comparado con la finalidad de plantear en el siguiente capítulo de esta investigación un proyecto de ley que recoja la tipificación de delitos informáticos.

## **2. Legislaciones comparadas**

### ***2.1. - Legislación de los Estados Unidos de América***

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

Con la finalidad de eliminar algunas definiciones de un virus informático, un gusano informático, un caballo de Troya informático y en que difieren de los virus, el acta de 1994 proscribe la transmisión de un programa, información, códigos o comandos que causan daños a la computadora, a los sistemas informáticos, a las redes, información, datos o programas (18 U.S.C.: Sec. 1030 (a) (5) (A)).

La ley penal comentada es un adelanto porque tipifica claramente los delitos de transmisión de virus informáticos. Diferencia el tratamiento a aquellos que de manera temeraria lanzan ataques de virus de aquellos que lo realizan con la intención de hacer estragos. Define dos niveles para el tratamiento de quienes crean virus:

- a) Para los que intencionalmente causan un daño por la transmisión de un virus, el castigo de hasta 10 años en prisión federal más una multa.
- b) Para los que lo transmiten sólo de manera imprudencial la sanción fluctúa entre una multa y un año en prisión.

El acta de 1994 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 materia de estafas electrónicas, defraudaciones y otros actos dolosos relacionados con los dispositivos de acceso a sistemas informáticos, la legislación estadounidense sanciona con pena de prisión y multa, a la persona que defraude a otro mediante la utilización de una computadora o red informática.

## **2.2. - Legislación de la Comunidad Económica Europea.<sup>86</sup>**

---

### **Documento 399D0276**

Decisión nº 276/1999/CE del Parlamento Europeo y del Consejo de 25 de enero de 1999 por la que se aprueba un plan plurianual de acción comunitaria para propiciar una mayor seguridad en la utilización de Internet mediante la lucha contra los contenidos ilícitos y nocivos en las redes mundiales.

**Diario Oficial nº L 033 de 06/02/1999 P. 0001 – 0011.**

DECISIÓN Nº 276/1999/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 25 de enero de 1999 por la que se aprueba un plan plurianual de acción comunitaria para propiciar una mayor seguridad en la utilización de Internet mediante la lucha contra los contenidos ilícitos y nocivos en las redes mundiales.

EL PARLAMENTO EUROPEO Y EL CONSEJO DE LA UNIÓN EUROPEA,

HA ADOPTADO LA PRESENTE DECISIÓN:

### **Artículo 1**

1. -. Se aprueba el plan plurianual de acción comunitaria para propiciar una mayor seguridad en la utilización de Internet (denominado en lo sucesivo el plan de acción), tal como se describe en el anexo I.

2. El plan de acción abarcará un período de cuatro años, desde el 1 de enero de 1999 hasta el 31 de diciembre de 2002.

3. La dotación financiera para la ejecución del plan de acción para el período comprendido entre el 1 de enero de 1999 y el 31 de diciembre de 2002 será de 25 millones de euros.

La Autoridad Presupuestaria autorizará los créditos anuales ajustándose a las perspectivas financieras.

En el anexo II figura un desglose indicativo del gasto.

### **Artículo 2**

El plan de acción tiene el objetivo de propiciar una mayor seguridad en la utilización de Internet y fomentar a nivel europeo la creación de un entorno favorable para el desarrollo de la industria vinculada a Internet.

### **Artículo 3**

Para cumplir el objetivo mencionado en el artículo 2, se llevarán a cabo las acciones siguientes de apoyo y promoción de las medidas que adopten los Estados miembros bajo la dirección de la Comisión y, de conformidad con las líneas de actuación que se establecen en el anexo I y los medios de ejecución del plan de acción que se establecen en el anexo III:

- fomentar la autorregulación del sector y los mecanismos de supervisión de los contenidos (por ejemplo, los relativos a contenidos tales como la pornografía infantil o aquellos que inciten al odio por motivos de raza, sexo, religión, nacionalidad u origen étnico).

- alentar al sector a ofrecer medios de filtro y sistemas de clasificación que permitan a padres y profesores seleccionar los contenidos apropiados para la educación de los menores a su cargo, y

---

<sup>86</sup> Legislación Europea Comunitaria, Documento 399D0276 <http://europa.eu.int/eur-lex/es/lif/index.html>

a los adultos decidir a qué contenidos lícitos desean tener acceso, y que tengan en cuenta la diversidad cultural y lingüística,

- mejorar entre los usuarios el conocimiento de los servicios ofrecidos por el sector, especialmente entre padres, educadores y menores, para que puedan entender y aprovechar mejor las oportunidades que ofrece Internet,
- llevar a cabo medidas de apoyo como la evaluación de las implicaciones jurídicas,
- realizar actividades para fomentar la cooperación internacional de los campos mencionados,
- efectuar otras actividades que contribuyan a la consecución de los objetivos establecidos en el artículo 2.

#### **Artículo 4**

1. La Comisión será responsable de la ejecución del plan de acción.

2. El procedimiento que se establece en el artículo 5 se aplicará a:

- el programa de trabajo, incluido todo gasto en las actividades descritas en el punto 9 del anexo III
- el desglose de los gastos presupuestarios,
- los criterios y contenidos de las convocatorias de propuestas,
- la evaluación de los proyectos presentados con arreglo a las convocatorias de propuestas para su financiación por la Comunidad y del importe estimado de la aportación comunitaria a cada proyecto cuando dicho importe sea igual o superior a 300 000 euros,
- las medidas para la evaluación del programa,
- cualquier apartamiento de las reglas que se establecen en el anexo III,
- la participación en cualquier proyecto de personas jurídicas de terceros países y de las organizaciones internacionales mencionadas en el apartado 3 del artículo 7,
- otras acciones que pudieran emprenderse conforme a lo dispuesto en el último guión del artículo 3.

3. Cuando, según lo previsto en el cuarto guión del apartado 2, el importe de la aportación comunitaria sea inferior a 300 000 euros, la Comisión informará al Comité contemplado en el artículo 5 sobre los proyectos y los resultados de su evaluación.

4. La Comisión informará periódicamente al Comité contemplado en el artículo 5 de los avances en la ejecución del programa en su conjunto.

#### **Artículo 5**

La Comisión estará asistida por un Comité compuesto por representantes de los Estados miembros y presidido por el representante de la Comisión.

El representante de la Comisión presentará al Comité un proyecto de las medidas que deban tomarse. El Comité emitirá su dictamen sobre dicho proyecto en un plazo que el presidente podrá determinar en función de la urgencia de la cuestión de que se trate. El dictamen se emitirá según la mayoría prevista en apartado 2 del artículo 148 del Tratado para adoptar aquellas decisiones que el Consejo deba tomar a propuesta de la Comisión. Los votos de los representantes de los Estados miembros en el seno del Comité se ponderarán de la manera definida en el artículo anteriormente citado. El presidente no tomará parte en la votación.

La Comisión adoptará las medidas previstas cuando sean conformes al dictamen del Comité. Cuando las medidas previstas no sean conformes al dictamen del Comité o en caso de ausencia de dictamen, la Comisión someterá sin demora al Consejo una propuesta relativa a las medidas que deban tomarse. El Consejo se pronunciará por mayoría cualificada. Si, transcurrido un plazo de tres meses a partir del momento en que la propuesta se haya sometido al Consejo, éste no se hubiere pronunciado, la Comisión adoptará las medidas propuestas.

#### **Artículo 6**

1. Para garantizar la utilización eficaz de la ayuda comunitaria, la Comisión velará por que las acciones emprendidas con arreglo a la presente Decisión estén de manera efectiva sujetas a valoración previa, supervisión y evaluación posterior.

2. Durante la ejecución de los proyectos y una vez concluidos, la Comisión evaluará la forma en que se han llevado a cabo y su impacto, para determinar si se han alcanzado los objetivos iniciales. 3. Los beneficiarios deberán presentar un informe anual a la Comisión. 4. Transcurrido un período de dos años y al concluir el plan de acción, la Comisión presentará al Parlamento Europeo, al Consejo, al Comité Económico y Social y al Comité de las Regiones, previo examen por el Comité contemplado en el artículo 5, un informe de evaluación de los resultados de la ejecución de las líneas de actuación enunciadas en el anexo I. Deberá hacerse referencia a las

conclusiones generales aplicables a todas las categorías de contenidos ilícitos. La Comisión podrá presentar, con arreglo a dichos resultados, propuestas para reorientar el plan de acción.

#### **Artículo 7**

1. Podrán participar en el plan de acción personas jurídicas establecidas en los Estados de la AELC que sean Estados miembros del Espacio Económico Europeo (EEE) de conformidad con lo dispuesto en el Acuerdo EEE. 2. Asimismo podrán participar personas jurídicas establecidas en Estados asociados de Europa Central y Oriental, de conformidad con las condiciones establecidas en los protocolos adicionales de los acuerdos de asociación, entre otras las de tipo financiero y las relativas a la participación en programas comunitarios. También podrán participar personas jurídicas establecidas en Chipre sobre la base de los créditos suplementarios y con arreglo a la misma normativa que se aplica en los Estados de la AELC miembros del EEE, de conformidad con los procedimientos que se acuerden con dicho país. 3. Podrán participar, de conformidad con el procedimiento establecido en el artículo 5 y sin asistencia financiera de la Comunidad en el marco del plan de acción, personas jurídicas establecidas en otros terceros países y organizaciones internacionales, cuando su participación contribuya de manera eficaz a la ejecución del plan de acción y teniendo en cuenta el principio de beneficio mutuo.

#### **Artículo 8**

Los destinatarios de la presente Decisión serán los Estados miembros.  
Hecho en Bruselas, el 25 de enero de 1999.

#### **2.2.1. - Legislación del Reino de España<sup>87</sup>:**

En el nuevo Código Penal español (aprobado por la Ley Orgánica 10/1995, de 23 de Noviembre / BOE (boletín Oficial Español) número 281, de 24 de Noviembre de 1.995 se encuentran varios artículos relacionados con los delitos informáticos, de esta forma procedemos a transcribirlos:

#### **Artículo 197. -**

1. - El que para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.

2. - Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero.

3. - Se impondrá la pena de prisión de dos a cinco años si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores. Será castigado con las penas de prisión de uno a tres años y multa de doce a veinticuatro meses, el que, con conocimiento de su origen ilícito y sin haber tomado parte en su descubrimiento, realizare la conducta descrita en el párrafo anterior.

4. - Si los hechos descritos en los apartados 1 y 2 de este artículo se realizan por las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros, se impondrá la pena de prisión de tres a cinco años, y si se difunden, ceden o revelan los datos reservados, se impondrá la pena en su mitad superior.

5. - Igualmente, cuando los hechos descritos en los apartados anteriores afecten a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o

---

<sup>87</sup> El texto completo del Código Penal Español puede verse en:  
<http://www.law.unican.es/incade/lex/cpint.htm>, del Instituto Cántabro de Derecho.

la víctima fuere un menor de edad o un incapaz, se impondrán las penas previstas en su mitad superior.

6. - Si los hechos se realizan con fines lucrativos, se impondrán las penas respectivamente previstas en los apartados 1 al 4 de este artículo en su mitad superior. Si además afectan a datos de los mencionados en el apartado 5, la pena a imponer será la de prisión de cuatro a siete años.

#### **Artículo 198. -**

La autoridad o funcionario público que, fuera de los casos permitidos por la Ley, sin mediar causa legal por delito, y prevaleciendo de su cargo, realizare cualquiera de las conductas descritas en el artículo anterior, será castigado con las penas respectivamente previstas en el mismo, en su mitad superior y, además, con la de inhabilitación absoluta por tiempo de seis a doce años.

#### **Artículo 199. -**

1. - El que revelare secretos ajenos, de los que tenga conocimiento por razón de su oficio o sus relaciones laborales, será castigado con la pena de prisión de uno a tres años y multa de seis a doce meses.

2. - El profesional que, con incumplimiento de su obligación de sigilo o reserva, divulgue los secretos de otra persona, será castigado con la pena de prisión de uno a cuatro años, multa de doce a veinticuatro meses e inhabilitación especial para dicha profesión por tiempo de dos a seis años.

#### **Artículo 200. -**

Lo dispuesto en este capítulo será aplicable al que descubriere, revelare o cediere datos reservados de personas jurídicas, sin el consentimiento de sus representantes, salvo lo dispuesto en otros preceptos de este código.

#### **Artículo 201. -**

1. - Para proceder por los delitos previstos en este capítulo será necesaria denuncia de la persona agraviada o de su representante legal. Cuando aquélla sea menor de edad, incapaz o una persona desvalida, también podrá denunciar el Ministerio Fiscal.

2. - No será precisa la denuncia exigida en el apartado anterior para proceder por los hechos descritos en el artículo 198 de este Código, ni cuando la comisión del delito afecte a los intereses generales o a una pluralidad de personas.

3. - El perdón del ofendido o de su representante legal, en su caso, extingue la acción penal o la pena impuesta, sin perjuicio de lo dispuesto en el segundo párrafo del número 4º del artículo 130.

#### **Artículo 211. -**

La calumnia y la injuria se reputarán hechas con publicidad cuando se propaguen por medio de la imprenta, la radiodifusión o por cualquier otro medio de eficacia semejante.

#### **Artículo 212. -**

En los casos a los que se refiere el artículo anterior, será responsable civil solidaria la persona física o jurídica propietaria del medio informativo a través del cual se haya propagado la calumnia o injuria.

#### **Artículo 238. -**

Son reos del delito de robo con fuerza en las cosas los que ejecuten el hecho cuando concurra alguna de las circunstancias siguientes:

1º. - Escalamiento.

2º. - Rompimiento de pared, techo o suelo, o fractura de puerta o ventana.

3º. - Fractura de armarios, arcas u otra clase de muebles u objetos cerrados o sellados, o forzamiento de sus cerraduras o descubrimiento de sus claves para sustraer su contenido, sea en el lugar del robo o fuera del mismo.

4º. - Uso de llaves falsas.

5º. - Inutilización de sistemas específicos de alarma o guarda.

**Artículo 239. -**

Se considerarán llaves falsas:

1º. - Las ganzúas u otros instrumentos análogos. 2º. - Las llaves legítimas perdidas por el propietario u obtenidas por un medio que constituya infracción penal. 3º. - Cualesquiera otras que no sean las destinadas por el propietario para abrir la cerradura violentada por el reo.

A los efectos del presente artículo, se consideran llaves las tarjetas, magnéticas o perforadas, y los mandos o instrumentos de apertura a distancia.

**Artículo 248. -**

1. - Cometen estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno.

2. - También se consideran reos de estafa los que, con ánimo de lucro, y valiéndose de alguna manipulación informática o artificio semejante consigan la transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero.

**Artículo 255. -**

Será castigado con la pena de multa de tres a doce meses el que cometiere defraudación por valor superior a cincuenta mil pesetas, utilizando energía eléctrica, gas, agua, telecomunicaciones u otro elemento, energía o fluido ajenos, por alguno de los medios siguientes:

1º. - Valiéndose de mecanismos instalados para realizar la defraudación.

2º. - Alterando maliciosamente las indicaciones o aparatos contadores.

3º. - Empleando cualesquiera otros medios clandestinos.

**Artículo 256. -**

El que hiciere uso de cualquier equipo terminal de telecomunicación, sin consentimiento de su titular, ocasionando a éste un perjuicio superior a cincuenta mil pesetas, será castigado con la pena de multa de tres a doce meses.

**Artículo 263. -**

El que causare daños en propiedad ajena no comprendidos en otros Títulos de este Código, será castigado con la pena de multa de seis a veinticuatro meses, atendidas la condición económica de la víctima y la cuantía del daño, si éste excediera de cincuenta mil pesetas.

**Artículo 264. -**

1. - Será castigado con la pena de prisión de uno a tres años y multa de doce a veinticuatro meses el que causare daños expresados en el artículo anterior, si concurriera alguno de los supuestos siguientes:

1º. - Que se realicen para impedir el libre ejercicio de la autoridad o en venganza de sus determinaciones, bien se cometiere el delito contra funcionarios públicos, bien contra particulares que, como testigos o de cualquier otra manera, hayan contribuido o pueden contribuir a la ejecución o aplicación de las Leyes o disposiciones generales.

2º. - Que se cause por cualquier medio infección o contagio de ganado.

3º. - Que se empleen sustancias venenosas o corrosivas.

4º. - Que afecten a bienes de dominio o uso público o comunal.

5º. - Que arruinen al perjudicado o se le coloque en grave situación económica.

2. - La misma pena se impondrá al que por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos.

**Artículo 270. -**

Será castigado con la pena de prisión de seis meses a dos años o de multa de seis a veinticuatro meses quien, con ánimo de lucro y en perjuicio de tercero, reproduzca, plagie, distribuya o comunique públicamente, en todo o en parte, una obra literaria, artística o científica, o su transformación, interpretación o ejecución artística fijada en cualquier tipo de soporte comunicada a través de cualquier medio, sin la autorización de los titulares de los correspondientes derechos de propiedad intelectual o de sus cesionarios.

La misma pena se impondrá a quien intencionadamente importe, exporte o almacene ejemplares de dichas obras o producciones o ejecuciones sin la referida autorización.

Será castigada también con la misma pena la fabricación, puesta en circulación y tenencia de cualquier medio específicamente destinada a facilitar la supresión no autorizada o la neutralización de cualquier dispositivo técnico que se haya utilizado para proteger programas de ordenador.

**Artículo 278. -**

1. - El que, para descubrir un secreto de empresa se apoderare por cualquier medio de datos, documentos escritos o electrónicos, soportes informáticos u otros objetos que se refieran al mismo, o empleare alguno de los medios o instrumentos señalados en el apartado 1 del artículo 197, será castigado con la pena de prisión de dos a cuatro años y multa de doce a veinticuatro meses.
2. - Se impondrá la pena de prisión de tres a cinco años y multa de doce a veinticuatro meses si se difundieren, revelaren o cedieren a terceros los secretos descubiertos.
3. - Lo dispuesto en el presente artículo se entenderá sin perjuicio de las penas que pudieran corresponder por el apoderamiento o destrucción de los soportes informáticos.

**Artículo 400. -**

La fabricación o tenencia de útiles, materiales, instrumentos, sustancias, máquinas, programas de ordenador o aparatos, específicamente destinados a la comisión de los delitos descritos en los capítulos anteriores, se castigarán con la pena señalada en cada caso para los autores.

**Artículo 536. -**

La autoridad, funcionario público o agente de éstos que, mediando causa por delito, interceptare las telecomunicaciones o utilizare artificios técnicos de escuchas, transmisión, grabación o reproducción del sonido, de la imagen o de cualquier otra señal de comunicación, con violación de las garantías constitucionales o legales, incurrirá en la pena de inhabilitación especial para empleo o cargo público de dos a seis años.

Si divulgare o revelare la información obtenida, se impondrán las penas de inhabilitación especial, en su mitad superior y, además, la de multa de seis a dieciocho meses.

## **2.2.2. - Legislación de la República Federal de Alemania<sup>88</sup>.**

---

En la República Federal de Alemania, es el lugar de Europa donde se ha realizado las reformas legales pertinentes para incluir los delitos informáticos en el Código Penal, de allí que desde el 15 de mayo de 1986 entró en vigencia la segunda Ley contra la Criminalidad Económica, que contempla los siguientes delitos:

- Espionaje de datos.
- Estafa informática.
- Alteración de datos.
- Sabotaje informático.

Revisemos los artículos de la precitada Ley de Alemania:

**Parágrafo 202ª StGB: Espionaje de datos.**

1. - “ El que sin autorización se procure para sí o para terceros datos que no estén destinados a él y que se encuentren especialmente protegidos contra un acceso no autorizado, serán castigados con la privación de libertad de hasta tres años o con multa.
2. - Son datos en el sentido del parágrafo 1. - únicamente aquellos que estén almacenados o son transmitidos electrónica, magnéticamente o de otra forma no perceptible directamente”

**Parágrafo 263ª StGB: Estafa informática.**

---

<sup>88</sup> El texto completo del Código Penal Alemán en idioma inglés puede verse en: <http://wings.buffalo.edu/law/bclc/germind.htm> del Centro de Leyes Penales de Buffalo, Estados Unidos de América.

1. - "El que con intención de procurarse a sí mismo o a un tercero un beneficio patrimonial antijurídico, causare un perjuicio en el patrimonio de otro, determinado el resultado de una operación de proceso de datos mediante la incorrecta configuración del programa, el empleo de datos incorrectos o incompletos, el empleo no autorizado de datos o cualquier otra intervención ilegítima en el curso del proceso será sancionado con una pena de prisión de hasta cinco años o pena de multa.
2. - El párrafo 263, apartados 2 a 5, es aplicable en lo que corresponda"

#### **Parágrafo 269 StGB. Falsificación de datos probatorios**

1. - " El que, para producir un engaño en el tráfico jurídico, almacene o altere datos probatorios de tal modo que, de ser percibidos, resultare un documento no auténtico o falseado, o se sirva de datos almacenados o alterados del modo referido, será castigado con pena privativa de libertad de hasta cinco años o con pena de multa.
2. - La tentativa es punible
3. - Debe aplicarse el Parágrafo 267, Parágrafo 3.

#### **Parágrafo 303<sup>a</sup>. Alteración de Datos.**

1. -" El que, de modo antijurídico, borre, oculte, haga inutilizable o altere datos (Parágrafo 202<sup>a</sup>, Párrafo 2), será castigado con pena de prisión de hasta dos años o pena de multa.
2. - La tentativa es punible.

#### **Parágrafo 303. Sabotaje informático.**

1. - " El que perturbare un proceso de datos que sea de importancia esencial para una empresa o establecimiento industrial ajeno o para la administración.  
-Cometiendo un hecho de los referidos en el parágrafo 303<sup>a</sup>, párrafo 1, ó
2. - destruyendo, dañando, inutilizando, eliminando o alterando un equipo de proceso de datos o un soporte, será sancionado con pena de prisión de hasta cinco años o de multa.
2. - La tentativa es punible.

### **2.2.3 -Gran Bretaña.**

---

Debido a un caso de hacking en 1991, comenzó a regir en este país la Computer Misuse Act (Ley de Abusos Informáticos). Mediante esta ley el intento, exitoso o no, de alterar datos informáticos es penado con hasta cinco años de prisión o multas. Esta ley tiene un apartado que especifica la modificación de datos sin autorización. Los virus están incluidos en esa categoría. El liberar un virus tiene penas desde un mes a cinco años, dependiendo del daño que causen.

### **2.2.4. -Holanda.**

---

El 1º de Marzo de 1993 entró en vigencia la Ley de Delitos Informáticos, en la cual se penaliza el hacking, la utilización de servicios de telecomunicaciones evitando el pago total o parcial de dicho servicio, la ingeniería social (arte de convencer a la gente de entregar información que en circunstancias normales no entregaría), y la distribución de virus.

La distribución de virus está penada de distinta forma si se escaparon por error o si fueron liberados para causar daño. Si se demuestra que el virus se escapó por error, la pena no superará el mes de prisión; pero, si se comprueba que fueron liberados con la intención de causar daño, la pena puede llegar hasta los cuatro años de prisión.

## **2.2.5. - República de Francia.89**

El legislador francés creó nuevos tipos penales relacionados con la delincuencia informática, mediante la Ley No.88-19 relativa al Fraude Informático, y la insertó en el Código Penal Francés, bajo la denominación “ De ciertas infracciones en materia informática”

Revisemos ahora el texto de la ley referida:

### **Art.462-2 Código Penal. Acceso fraudulento a un sistema de elaboración de datos.**

“ Quien fraudulentamente acceda a todo o parte de un sistema de tratamiento automático de datos o se mantenga en él será castigado con prisión de dos meses a un año y con multa de 2.000 a 50.000 francos o con una de las dos penas.

Si de ello resulta la supresión o modificación de datos contenidos en un sistema o resulta la alteración del funcionamiento del sistema, la prisión será de dos meses a dos años y la multa de 10.000 a 100.000 francos.”

### **Art. 462-3 Código Penal.- Sabotaje informático.**

“ Quien, intencionalmente y con menosprecio de los derechos de los demás, impida o falsee el funcionamiento de un sistema de tratamiento automático de datos será castigado con prisión de tres meses a tres años y con multa de 10.000 francos o con una de las dos penas”

### **Art. 462-4 Código Penal.- Destrucción de datos**

“Quien intencionalmente 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 éste contiene o los modos de tratamiento o de transmisión, será castigado con prisión de tres meses a tres años y con multa de 2.000 a 500.000 francos o con una de las dos penas”

### **Art. 462-5 Código Penal.- Falsificación de documentos informáticos.**

“ Quien de cualquier modo falsifique documentos informatizados, con la intención de causar un perjuicio a otro, será castigado con prisión de un año a cinco años y con multa de 20.000 a 2'000.000 de francos, o con una de estas dos penas”

### **Art. 462-6 Código Penal. Uso de documentos informatizados falsos.**

“ Quien conscientemente haga uso de documentos falsos del Art. 462-5 será castigado con prisión de un año a cinco años y con multa de 20.000 a 2'000.000 de francos o con una de las dos penas ”

**Art. 462-7 Código Penal.-** Dispone que la tentativa se castiga con la misma pena que el delito mismo (o consumado)

**Art. 462-8 Código Penal.-** Sanciona a los que han participado en una asociación formada o en un acuerdo tendiente a la preparación o concreción por uno o varios hechos materiales, de uno o varios de estos delitos, con la pena más severa en ellos establecida.

**Art. 462-9 Código Penal.-** Este artículo faculta al tribunal para confiscar los materiales utilizados en la comisión de estos delitos, o que hayan servido para ello.”

---

<sup>89</sup> El texto completo del Código Penal francés puede revisarse en <http://www.legifrance.gouv.fr/citoyen/code.ow>

## **2.3. - Legislación de la República de Chile.<sup>90</sup>**

---

Chile fue el primer país latinoamericano en sancionar una Ley contra delitos informáticos, en vigencia desde el 7 de junio de 1993.

Revisemos el texto de la mencionada ley.

### **Ley No. 19.223**

#### **Artículo 1.**

El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento, sufrirá la pena de presidio menor en su grado medio a máximo Si como consecuencia de estas conductas se afectaren los datos contenidos en el sistema, se aplicará la pena señalada en el inciso anterior, en su grado máximo.

#### **Artículo 2.**

El que con ánimo de apoderarse, usar o conocer indebidamente la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio.

#### **Artículo 3.**

El que maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información, será castigado con presidio menor en su grado medio.

#### **Artículo 4.**

El que maliciosamente revele o difunda los datos contenidos en un sistema de información sufrirá la pena de presidio menor en su grado medio. Si quien incurriere en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado.

## **2.4. - Legislación de los Estados Unidos Mexicanos<sup>91</sup>.**

---

El único estado de los Estados Unidos Mexicanos que contempla en su legislación los delitos informáticos es el Estado de Sinaloa. Ante la importancia que tiene que el Congreso Local del Estado de Sinaloa haya legislado sobre la materia de delitos informáticos, consideramos pertinente transcribir íntegramente el texto que aparece en el Código Penal Estatal de Sinaloa.

### **Título Décimo.**

#### **Delitos contra el Patrimonio**

#### **Capítulo V Delito Informático**

#### **Artículo 217. -**

Comete delito informático, la persona que dolosamente y sin derecho:

- I. Use o entre a una base de datos, sistemas de computadores o red de computadoras o a cualquier parte de la misma, con el propósito de diseñar, ejecutar o alterar un esquema o artificio con el fin de defraudar, obtener dinero, bienes o información; o
- II. Intercepte, interfiera, reciba, use, altere, dañe o destruya un soporte lógico o programa de computadora o los datos contenidos en la misma, en la base, sistema o red.

---

<sup>90</sup> Texto de la Ley fue tomado desde el sitio electrónico: <http://www.v/lex.com>

<sup>91</sup> Código Penal del Estado de Sinaloa, en <http://www.v/lex.com>

Al responsable de delito informático se le impondrá una pena de seis meses a dos años de prisión y de noventa a trescientos días multa.

## **2.5. - Legislación de la República de Colombia.**

En la República de Colombia existen varias disposiciones legales relacionadas con la informática, sin embargo aún no se ha legislado sobre los delitos informáticos, de allí que revisaremos el proyecto de ley de reforma del Código Penal colombiano presentado por la Dra. María Fernanda Guerrero, Dr. Jaime Eduardo Santos, Dr. Víctor Zuluaga Hoyos entre otros destacados profesionales.<sup>92</sup>

“ Al Artículo 119 del Código Penal se adicionará el inciso segundo del siguiente tenor:

**Art.119.- Espionaje.-** El que indebidamente obtenga, emplee o revele secreto político, económico o militar, relacionado con la seguridad del Estado, incurrirá en prisión de tres (3) a doce (12) años. Si para la obtención, empleo, divulgación o transferencia de la información se utilizaren sistemas informáticos, telemáticos o satelitales o se accede a ellos violando las seguridades electrónicas, la pena se aumentará de una tercera parte a la mitad.”<sup>93</sup>

“Se modifica el inciso segundo art. 187, con el siguiente texto: **Terrorismo.-** Si el estado de zozobra o terror es provocada por llamada telefónica, cinta magnetofónica, video, cassettes o escrito anónimo, o por información o mensajes a través de cualquier medio electrónico, información y telemático la pena será de dos (2) a cinco (5) años y la multa de cinco (5) a cincuenta (50) salarios mínimos mensuales”<sup>94</sup>

El art. 225 del Código Penal quedará así:

“ **Art.225.- Otros documentos.-** Para efectos de los artículos anteriores se asimilan a documentos, siempre que pueda servir de prueba, las expresiones de persona conocida o conocible recogidas por cualquier medio mecánico, los planos, dibujos, cuadros, fotografías, cintas cinematográficas, radiografías, fonópticas, documentos informáticos que contengan datos, información y programas, registros en cuentas que se encuentren en cualquier soporte informático y para cuya eficacia probatoria se tendrán en cuenta los criterios de imputación e integridad del mismo.”<sup>95</sup>

“Se agregará al art. 228 el siguiente inciso: “ Para los efectos anteriores se tendrá como medio de prueba el documento informático que contengan datos e informaciones con eficacia probatoria o programas específicamente destinados a elaborarlos”.<sup>96</sup>

“ El Código Penal tendrá un artículo con el número 288<sup>a</sup> con el siguiente tenor: **Art. 288<sup>a</sup>.- Violación ilícita de comunicaciones informáticas y telemáticas.-** El que ilícitamente intercepte, sustraiga, oculte, extravíe, destruya, intercepte, controle, impida, interrumpa, altere o suprima información pública o privada dirigida a otra persona a través de la comunicación informática y telemática o de cualquier otra transmisión a distancia de imágenes y sonidos a través de datos incurrirá en arresto de seis (6) meses a dos (2) años siempre que el delito no constituya delito sancionado con pena mayor.”<sup>97</sup>

“ Adicionar el artículo 289<sup>a</sup> al Código Penal con el siguiente texto:

**Art.289<sup>a</sup> .- Acceso abusivo a un sistema informático o telemático.-** El que abusivamente se introduzca en un sistema informático o telemático protegido con medida de seguridad o se

<sup>92</sup> Guerrero, María Fernanda., Santos Jaime Eduardo, y otros. , “ Penalización de la criminalidad informática, proyecto académico”, Ed.Jurídica Gustavo Ibañez, Colombia, 1998.

<sup>93</sup> Ob.Cit. , pág.101

<sup>94</sup> Ob.Cit. , pág.108

<sup>95</sup> Ob.Cit. , pág.112

<sup>96</sup> Ob.Cit. , Pág., 112-113.

<sup>97</sup> Ob.Cit. , Pág., 122-123.

mantiene contra la voluntad expresa o tácita de quien tiene el derecho de excluirlo, incurrirá en prisión de seis (6) meses a tres (3) años y multa de uno a cien salarios mínimos vitales. La pena se aumentará de una tercera parte a la mitad si el acceso ilegal es cometido por un servidor público, por operador del sistema si se comete con violencia sobre las personas y las cosas o si del hecho se deriva la destrucción del sistema o se afecta considerablemente su funcionamiento.”<sup>98</sup>

“Adiciónase el artículo 289B al Código Penal con el siguiente texto: **Art.289. B.- Posesión y difusión abusiva de dispositivos de acceso a sistemas informáticos y telemáticos.-** El que con el fin de procurarse un provecho ilícito para sí o para un tercero, por cualquier medio obtenga, reproduzca, difunda o elabore y entregue códigos de acceso de acceso a sistemas informáticos o telemáticos protegidos con el propósito de violar sus seguridades, incurrirá en prisión de dos a cinco años.

Si las conductas anteriores se derivan un perjuicio económico para entidades públicas o privadas la pena se aumentará de una tercera parte a la mitad.”<sup>99</sup>

“Se modifica el numeral 4º. Del artículo 350 del Código Penal con el siguiente texto: **Art.350.- Hurto calificado. 4º.** - Con escalamiento, con llaves sustraídas o falsas, ganzúas, tarjetas, claves u otros dispositivos de acceso ilícitamente obtenidas, descifrando claves encriptadas u otros instrumentos similares o violando seguridades electrónica, informática u otras semejantes”<sup>100</sup>

“Se adiciona al artículo 352 del Código Penal un inciso segundo del siguiente tenor: **Art.352ª. - Hurto de uso de la memoria o del tiempo de máquina del computador.-** El que abusivamente utilice la memoria o del tiempo de máquina del computador siempre que el hecho no configure delito sancionado con una pena mayor la pena será de seis (6) meses a un (1) año de prisión.

La pena se aumentará de una tercera parte a la mitad si el agente aprovecha su calidad de operador de sistemas”<sup>101</sup>

“El Código Penal tendrá los artículos 356ª , 356B bajo el Capítulo III llamado de la estafa y el fraude informático con el siguiente tenor:

### CAPITULO III

#### DE LA ESTAFA Y EL FRAUDE INFORMÁTICO

**Art. 356ª. - Fraude informático.-** El que alterando de cualquier manera el funcionamiento de un sistema informático y telemático; o intervenga sin derecho en cualquier modalidad de datos, informaciones o programas contenidos en un sistema informático o telemático o que pertenezcan a ellos, procurándose para sí o para otros provecho ilícito y ocasionando daño a otros será sancionado con una pena de cuatro (4) a doce (12) años y multa de cien a doscientos salarios mínimos mensuales.

La pena se aumentará en una tercera parte a la mitad si el hecho se comete con abuso de la calidad de operador de sistemas.”<sup>102</sup>

“ **Art.358B.- Uso fraudulento de tarjetas u otros medios de pago análogos.-** El que con el fin de obtener beneficio para si o para otros indebidamente utiliza no siendo el titular tarjetas de crédito de pago, o cualquier otro documento análogo que habilite el retiro de dinero en efectivo o a la administración de bienes o la prestación de servicios será sancionado con una pena de prisión de uno (1) a cinco (5) años y con una multa de cien a mil salarios mínimos mensuales.

<sup>98</sup> Ob.Cit. , Pág., 123-124.

<sup>99</sup> Ob.Cit. , pág.124

<sup>100</sup> Ob.Cit. , Pág. 129, 130.

<sup>101</sup> Ob.Cit. , pág.131

<sup>102</sup> Ob.Cit. , pág.137

La misma pena se aplicará a quien con la intención de obtener provecho para sí o para un tercero falsifique o altere tarjetas de crédito o de pago o de cualquier otro documento análogo que permita el retiro de dinero en efectivo o la administración de bienes o servicios; O posea, ceda, adquiera tarjetas o documentos de procedencia ilícita o también falsificadas o alteradas así como las órdenes de pago producidas con ellas.”<sup>103</sup>

“El Código Penal tendrá el artículo 370<sup>a</sup> con el siguiente texto.-

**Art.370.- Daño en sistemas informáticos o telemáticos.-** El que destruya, deteriore, altere o haga inservible en todo o en parte sistemas informáticos y telemáticos, programas, informaciones o datos será sancionado salvo que el hecho no constituya delito sancionado con pena mayor de prisión de seis meses (6) meses a tres

(3) años y multa de cincuenta a doscientos salarios mínimos.

Si el hecho se cometiere abusando de la calidad de operador del sistema, la pena será de uno (1) a cuatro años (4) años y multa de cincuenta a cien salarios mínimos.

Si el hecho se deriva de la destrucción, cancelación, supresión de los elementos del sistema, de los datos o de la información o programas o hay una interrupción parcial del funcionamiento la pena será de seis meses (6) meses a tres (3) años y multa de diez a cien salarios mínimos.”<sup>104</sup>

## ***2.6. - Legislación de la República del Perú.***<sup>105</sup>

---

### **LEY QUE INCORPORA LOS DELITOS INFORMÁTICOS AL CÓDIGO PENAL.- LEY No. 27309**

Modifícase el Título V del Libro Segundo del Código Penal, promulgado por Decreto Legislativo No 635, con el texto siguiente:

#### **"TÍTULO V**

#### **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 cincuentidós 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

---

<sup>103</sup> Ob.Cit. , pág.137

<sup>104</sup> Ob.Cit., pág.143

<sup>105</sup> Las leyes de Perú pueden encontrarse en la siguiente dirección electrónica: <http://www.latinlex.com>

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.

### **CAPÍTULO XI**

#### **DISPOSICIÓN COMÚN**

#### **Artículo 208o. -**

No son reprimibles, sin perjuicio de la reparación civil, los hurtos, apropiaciones, defraudaciones o daños que se causen:

1. Los cónyuges, concubinos, ascendientes, descendientes y afines en línea recta.
2. El consorte viudo, respecto de los bienes de su difunto cónyuge, mientras no hayan pasado a poder de tercero.
3. Los hermanos y cuñados, si viviesen juntos”  
Dado en la Casa de Gobierno, en Lima, a los quince días del mes de julio del año dos mil.

## **3. - Organismos internacionales de prevención de delitos informáticos.**

En 1983 la Organización de Cooperación y Desarrollo Económico (OCDE) inició un estudio de la posibilidad de aplicar y armonizar en el plano internacional las leyes penales, a fin de luchar contra el problema del uso indebido de los programas de computación.

Las posibles implicaciones económicas de la delincuencia informática tienen carácter internacional, cuyo principal problema es la falta de una legislación unificada que, facilita la comisión de los delitos.

En 1986 la OCDE publicó un informe titulado Delitos de informática: análisis de la normativa jurídica, donde se reseñaban las normas legislativas vigentes y las propuestas de reforma en diversos Estados miembros y se recomendaba una lista mínima de ejemplos de uso indebido que los países podrían prohibir y sancionar en leyes penales.

En 1992 elaboró un conjunto de normas para la seguridad de los sistemas de información, con intención de ofrecer las bases para que los Estados y el sector privado pudieran erigir un marco de seguridad para los sistemas informáticos.

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

La ONU ha publicado una descripción de "Tipos de Delitos Informáticos"

En 1992 la Asociación Internacional de Derecho Penal durante el coloquio celebrado en Wurzburg en 1992, adoptó diversas recomendaciones respecto a los delitos informáticos, entre ellas que, en la medida que el Derecho Penal no sea suficiente, deberá promoverse la modificación de la definición de los delitos existentes o la creación de otros nuevos, si no basta con la adopción de otras medidas como por ejemplo el principio de subsidiariedad.

Las dificultades a la hora de encontrar pruebas y la no-coincidencia entre el lugar del delito y el lugar dónde se sufren sus consecuencias complican en gran manera el seguimiento de los delincuentes cibernéticos. Por este motivo las autoridades policiales de muchos países, como la policía británica de Scotland Yard<sup>106</sup> o el FBI, e incluso Interpol, han creado departamentos especializados en delincuencia informática, una especie de ciber policía.

Las organizaciones globales apoyadas en la burocracia exigen unos procesos tan lentos que hacían imposible una investigación válida de los delitos cibernéticos. En España, la Guardia Civil creó en 1996 la Unidad de Delitos Informáticos tras la aparición del nuevo Código Penal en el que, por primera vez, se tipificaban delitos relacionados con la informática.

---

<sup>106</sup> Puede verse las páginas en Internet en las siguientes direcciones: Scotland Yard: <http://www.met.police.uk/>, Federal Bureau Investigation <http://www.fbi.gov.>, Interpol <http://www.interpol.com>

# **CAPITULO V: PROPUESTA DE TIPIFICACIÓN DE DELITOS INFORMÁTICOS EN LA LEGISLACIÓN PENAL ECUATORIANA:**

## **1.- Ideas Generales**

La especial naturaleza de los datos digitalizados y de los programas de ordenador denominados como software, su carácter intangible, no le permite al tipo penal tradicional cubrirlo haciendo necesaria la creación de nuevos delitos.

Precisamente, el profesor chileno Renato Jijena Leiva <sup>107</sup>sostiene esta postura. El tratadista citado piensa que la especial naturaleza de los programas de ordenadores no les permite estar ni siquiera incluidos en una clasificación tan general como la de cosas corporales e incorpóreas. Si definimos a los programas computacionales como un conjunto de instrucciones para ser usadas en un computador, no podrán ser percibidas por los sentidos, y por ende, no son cosas corporales. Y tampoco consisten en meros derechos, es decir, no son cosas incorpóreas. Se trataría de meros impulsos electromagnéticos que se transmiten a través de circuitos electrónicos no perceptibles por los sentidos del hombre (ya que lo que se observa en un monitor es el resultado obtenido con el procesamiento electrónico de las instrucciones).

Al ser intangibles e inmateriales no se pueden aprehender físicamente, es más, al copiarlos ilegalmente no le son privados en forma permanente a la víctima del delito. Sólo una nueva figura delictiva, es decir, un delito informático, podría sancionar penalmente tales conductas.

Examinemos ahora los interrogantes para los tratadistas del Derecho Penal Internacional ya que se deberá resolver las complejas situaciones que se generan a partir del accionar de los delincuentes informáticos teniendo en cuenta que, en la mayoría de los casos, se trata de delitos a distancia. Supongamos que un país cualquiera modifica su código penal e incluye en éste como delito al acceso no autorizado a sistemas de información. Luego, varios computadores de una entidad financiera sufren un acceso no autorizado tendiente a obtener una transferencia indebida, se descubre quien accede, pero resulta que el violador del sistema es un suizo que vive en Australia y que penetró en el sistema a través de un servidor que se encuentra en Ecuador. La pregunta inevitable es: ¿podría el Estado en cuestión arrogarse la potestad de persecución del delito?

A fin de brindar alguna solución, hay autores que consideran que el juez penal puede intervenir por la sola circunstancia de que la infracción fue cometida en el territorio de su país. En pocas palabras, es el vínculo del territorio el que justifica la aplicación de la ley penal.

Estimamos que si se apunta a una correcta legislación deberán arbitrase, además, los mecanismos que permitan la repercusión fuera del territorio nacional.

El delito sobre elementos informáticos ha presentado dos problemas en la aplicación. Por un lado, la regulación casuística, y por otro, el ajuste de la pena al valor de lo que ha sido destruido. En ocasiones los perjuicios pueden llegar a ser muy elevados, mientras que el valor de lo destruido es bastante bajo.

---

<sup>107</sup> JIJENA LEIVA, Renato Javier., Ob.Cit., pág. 169 y ss.

Para la correcta aplicación de las normas penales que castiguen los delitos informáticos se requiere dentro del proceso penal las herramientas adecuadas para investigar, identificar, y procesar con éxito a delincuentes del ordenador. Los delitos informáticos de hoy, no se pueden investigar con eficacia con los dispositivos procesales del siglo pasado.

Los delitos informáticos presentan nuevos desafíos para investigación jurídica en todos los niveles, como por ejemplo la jurisdicción y competencia de los Jueces y Tribunales que deban juzgar al delincuente informático, la responsabilidad del menor de edad, la coordinación y preparación del personal que integra varios organismos estatales; Fuerza Pública, Ministerio Fiscal, Función Judicial, Función Ejecutiva, Función Legislativa.

Se propone que lo más adecuado es tipificar en el Código Penal los nuevos delitos que surgen del mal uso que se le da a las tecnologías de la información y que por sus características no puedan encuadrarse dentro de los delitos tradicionales.

## **2.- Delitos contemplados en la ley de propiedad intelectual de la República del Ecuador.**

### **Capítulo III DE LOS DELITOS Y DE LAS PENAS**

**Art. 320.-** Serán reprimidos con igual pena que la señalada en el artículo anterior, quienes en violación de los derechos de propiedad intelectual:

1. Divulguen, adquieran o utilicen secretos comerciales, secretos industriales o información confidencial;

**Art. 324.-** Serán reprimidos con prisión de tres meses a tres años y multa de quinientas a cinco mil unidades de valor constante (UVC), tomando en consideración el valor de los perjuicios ocasionados, quienes en violación de los derechos de autor o derechos conexos:

a) Alteren o mutilen una obra, inclusive a través de la remoción o alteración de información electrónica sobre el régimen de derechos aplicables;

c) Reproduzcan una obra;

d) Comuniquen públicamente obras, videogramas o fonogramas, total o parcialmente;

e) Introduzcan al país, almacenen, ofrezcan en venta, vendan, arrienden o de cualquier otra manera pongan en circulación o a disposición de terceros reproducciones ilícitas de obras;

f) Reproduzcan un fonograma o videograma y en general cualquier obra protegida, así como las actuaciones de intérpretes o ejecutantes, total o parcialmente, imitando o no las características externas del original, así como quienes introduzcan al país, almacenen, distribuyan, ofrezcan en venta, vendan, arrienden o de cualquier otra manera pongan en circulación o a disposición de terceros tales reproducciones ilícitas; y,

**Art. 325.-** Serán reprimidos con prisión de un mes a dos años y multa de doscientos cincuenta a dos mil quinientas unidades de valor constante (UVC), tomando en consideración el valor de los perjuicios ocasionados, quienes en violación de los derechos de autor o derechos conexos:

a) Reproduzcan un número mayor de ejemplares de una obra que el autorizado por el titular;

b) Introduzcan al país, almacenen, ofrezcan en venta, vendan, arrienden o de cualquier otra manera pongan en circulación o a disposición de terceros reproducciones de obras en número que exceda del autorizado por el titular;

c) Retransmitan por cualquier medio las emisiones de los organismos de radiodifusión; y,

d) Introduzcan al país, almacenen, ofrezcan en venta, vendan, arrienden o de cualquier otra manera pongan en circulación o a disposición de terceros aparatos u otros medios destinados a descifrar o decodificar las señales codificadas o de cualquier otra manera burlar o quebrantar los medios técnicos de protección aplicados por el titular del derecho.

**Art. 328.-** Las infracciones determinadas en este capítulo son punibles y pesquisables de oficio.

**Art. 329.-** Las acciones civiles y penales prescriben de conformidad con las normas del Código Civil y del Código Penal, respectivamente, salvo las acciones por violación a los derechos morales, que son imprescriptibles.

Salvo prueba en contrario y, para los efectos de la prescripción de la acción, se tendrá como fecha de cometimiento de la infracción, el primer día del año siguiente a la última edición, reedición, reproducción, comunicación, u otra utilización de una obra, interpretación, producción o emisión de radiodifusión.

**Art. 330.-** En todos los casos comprendidos en este capítulo, se dispondrá el comiso de todos los objetos que hubieren servido directa o indirectamente para la comisión del delito, cuyo secuestro podrá ser ordenado por el juez penal en cualquier momento durante el sumario y obligatoriamente en el auto de apertura del plenario.

**Art. 331.-** El producto de las multas determinadas en este capítulo será destinado en partes iguales a la Función Judicial y al IEPI, el que lo empleará al menos en un cincuenta por ciento, en programas de formación y educación sobre propiedad intelectual.

Luego de transcribir los artículos que en nuestro criterio se encuentran vinculados con los delitos informáticos es necesario realizar el siguiente comentario. Las leyes en materia de propiedad intelectual son muy necesarias para tutelar los derechos de autor, de marcas y patentes, sin embargo la utilización de la Red Internet y las Nuevas Tecnologías de Información, hacen que personas de cualquier lugar del planeta, cometa los delitos que se han tipificado en la Ley de Propiedad Intelectual.

Por ejemplo el artículo 325 literal d) dice: , Introduzcan al país, almacenen, ofrezcan en venta, vendan, arrienden o de cualquier otra manera pongan en circulación o a disposición de terceros aparatos u otros medios destinados a descifrar o decodificar las señales codificadas o de cualquier otra manera burlar o quebrantar los medios técnicos de protección aplicados por el titular del derecho. El programa electrónico denominado NAPSTER<sup>108</sup> está diseñado para establecer una comunicación electrónica entre ordenadores de todo el mundo con la finalidad de copiar piezas musicales en formato digital denominado MP3, con lo que se estuvo, está y estará vulnerando los derechos de autor de cientos de miles de composiciones musicales. El sitio NAPSTER ha sido demandado en varios países del mundo por varias compañías pertenecientes a la industria discográfica.

Se hizo presente durante la discusión de la ley, ideas tales como, que al tratarse de una legislación codificada, la tendencia de los legisladores debería fortalecerla y no seguir creando legislaciones penales particulares y especiales que sólo sirven para desperdigar la normativa penal existente, lo que dificulta la labor del juez y la defensa de los inculpados, de esta forma la ubicación del texto correspondiente a los artículos señalados anteriormente y que constan en la Ley de Propiedad Intelectual ecuatoriana fuera del Código Penal es una desafortunada técnica legislativa.

---

<sup>108</sup> En los momentos en que se escribe este párrafo, los representantes legales de NAPSTER, han solicitado la apelación al fallo judicial por el que se les impedía poner a disposición de los cibernautas el programa NAPSTER. Sin embargo se puede acceder al sitio desde varios lugares en el Internet.

### **3.- PROYECTO DE LEY QUE CONTEMPLA LOS DELITOS INFORMÁTICOS**

#### **EXPOSICIÓN DE MOTIVOS**

A comienzos del siglo XXI la materialización de la idea del mundo como aldea global, el ciberespacio y el impacto de las Ciencias de la Informática y de las Nuevas Tecnologías han implicado una transformación en la forma de convivir en la sociedad.

Dentro de este marco de transformación, el cambio producido por el mal uso de la informática y de los ordenadores y/o computadores han hecho que surjan nuevas conductas merecedoras del reproche social. Así han surgido modalidades delictivas relacionadas con la informática.

En primer lugar, ciertas figuras típicas penales han comenzado a sobrevenir mediante el empleo de la tecnología de la información, es decir, ha comenzado a ser utilizada la informática como un medio de comisión específico.

Dichas conductas pueden ser comprendidas dentro del tipo penal del delito produciéndose una informatización de un ilícito tradicional.

Pero además han surgido nuevas conductas, impensadas por el legislador de hasta hace un cuarto de siglo, que por su especial naturaleza no admiten encuadrarse dentro de figuras convencionales penales sino que es necesario que se creen nuevos tipos. Son estos nuevos delitos a los que se les denomina delitos informáticos.

Resulta innegable que estas nuevas conductas tienen un enorme impacto en la sociedad, de esta forma causan perjuicios a terceros a veces en forma indeterminada, por ejemplo, perjudicando a bancos de datos en poder de organismos del Estado ecuatoriano.

#### **CONGRESO NACIONAL**

##### **CONSIDERANDO:**

-QUE, la Constitución Política de la República del Ecuador en su artículo 80 establece como deber fundamental del Estado el fomentar la ciencia y tecnología, así como garantizar la libertad de dichas actividades y la protección legal de sus resultados;

-QUE, el desarrollo de las Ciencias de la Informática y de las Nuevas Tecnologías han abierto la puerta a conductas antisociales y delictivas que se manifiestan en formas que hasta ahora no era posible imaginar.

- QUE, es necesario tutelar los derechos de los ciudadanos que se menoscaban con el cometimiento de los denominados delitos informáticos, y de esta forma contemplar en el Código Penal ecuatoriano vigente las nuevas figuras delictivas ya que, de no hacerlo, la ausencia de figuras especialmente tipificadas daría lugar a que los autores, cómplices y encubridores de éstos ilícitos quedaran sin sanción penal;

-QUE, por estas consideraciones es necesario que se atiendan y regulen las cada vez más frecuentes consecuencias del uso indebido de los ordenadores y de los sistemas informáticos, a través de los delitos informáticos, que han sido reconocidos en la legislación penal de varios países del mundo;

En uso de sus atribuciones expide la presente:

## LEY QUE REFORMA EL CÓDIGO PENAL ECUATORIANO<sup>108a</sup>

Agréguese el siguiente Título, después del Título X del Código Penal que dirá:

### TITULO XI DE LAS INFRACCIONES INFORMÁTICAS

**Art.- .... FRAUDE INFORMÁTICO.-** Son responsables de fraude informático la persona o personas que con ánimo de lucro y valiéndose de cualquier método o medio, alteren, manipulen, o modifiquen el funcionamiento de un programa informático, sistema informático, telemático, o un mensaje de datos para procurarse para sí o para otros un activo patrimonial de otra persona, en perjuicio de ésta o de un tercero, serán sancionados con pena de prisión de uno a cinco años y con multa de 1.000 a 10.000 dólares o con una de estas dos penas.

La pena indicada en el inciso anterior será impuesta al máximo establecido, si la persona que cometiere el delito tipificado en el párrafo anterior, lo comete en razón de su empleo u oficio.

**Art.- ... DAÑOS INFORMÁTICOS.-** Son responsables del delito de daños informáticos, la persona o personas que utilizando cualquier método o medio destruyan, alteren, deteriore, inutilicen, supriman o dañen: datos, bases de datos, programas informáticos, documentos electrónicos o cualquier mensaje de datos contenido en cualquier soporte lógico, sistema informático, o telemático; y serán reprimidas con reclusión menor de tres a seis años y con multa de 3.000 a 15.000 dólares o con una de estas dos penas.

La pena indicada en el inciso anterior será impuesta al máximo establecido, si la persona que cometiere el delito tipificado en el párrafo anterior, lo comete en razón de su empleo u oficio.

**Art.- ... DE LA FALSIFICACIÓN INFORMÁTICA.-** son responsables de falsificación informática la persona o personas que con ánimo de lucro, o bien para causar un perjuicio a un tercero, utilizando cualquier medio alteren o modifiquen documentos electrónicos, o la información incluida en éstos, que se encuentre contenida en cualquier soporte material, sistema informático o telemático, ya sea:

- 1.- Alterando un mensaje de datos en alguno de sus elementos o requisitos de carácter esencial.
- 2.- Simulando un mensaje de datos en todo o en parte, de manera que induzca a error sobre su autenticidad.
- 3.- Suponiendo en un acto, la intervención de personas que no la han tenido, o atribuyendo a las personas que han intervenido en él declaraciones o manifestaciones diferentes de las que hubieren hecho.
- 4.- Faltando a la verdad en la narración de los hechos.

Cualquier alteración, falsificación, simulación, falsa suposición o imputación de un mensaje de datos. Será reprimido con reclusión menor ordinaria de seis a nueve años y multa de 15.000 a 25.000 dólares o con una de estas dos penas.

Si la infracción de falsificación informática es cometida por un funcionario público, la pena será de reclusión menor extraordinaria de 9 a 12 años y multa de 25.000 a 50.000 o con una de estas dos penas y además traerá consigo la inhabilidad permanente de ocupar un cargo público.

### ART.-.... DE LA INSTRUSIÓN INDEBIDA A LOS SISTEMAS INFORMÁTICOS, DE INFORMACIÓN O TELEMÁTICOS..-

---

<sup>108a</sup> Se ha tomado como base el proyecto de ley de comercio electrónico y firmas electrónicas en lo que se refiere a las infracciones informáticas. Nuestros sinceros agradecimientos al Lcdo. Santiago Acurio, autor de las infracciones informáticas, en el referido proyecto de ley, por compartir sus estudios sobre el tema motivo de esta investigación.

Son responsables de intrusión indebida a los sistemas informáticos o telemáticos la persona o personas que por cualquier medio o fin y con el ánimo de apoderarse de la información contenida en dichos sistemas, o para descubrir los secretos comerciales o industriales o bien para vulnerar la intimidad, de una persona natural o jurídica, sin su consentimiento o autorización, interfieran, interrumpen, intercepten o se apoderen de cualquier mensaje de datos. Serán reprimidos con prisión de uno a cinco años y multa de 1.000 a 10.000 dólares o con una de estas dos penas.

Si la divulgación o la utilización fraudulenta de la información reservada, los secretos comerciales o industriales, han sido obtenidos por alguna de las formas indicadas en el párrafo anterior será sancionada con pena de reclusión menor de tres a seis años y multa de 3.000 a 15.000 dólares o con una de estas dos penas.

Si la divulgación o la utilización fraudulenta de la información reservada, los secretos comerciales o industriales, se realiza por la persona o personas a las cuales se les encomendó su custodia o utilización serán sancionadas con una pena de reclusión menor extraordinaria de nueve a doce años y con multa 25.000 a 50.000 o con una de estas dos penas y además traerá consigo la inhabilidad permanente de ocupar un cargo público o el cargo al cual pertenecía.

**ART.-...RECOPIACIÓN DE INFORMACIÓN NO AUTORIZADA:** En caso de que una persona o personas recopilaran por medios fraudulentos datos o información nominativa personal, para después cederla, utilizarla o transferirla a cualquier título sin la autorización de su titular o titulares, serán sancionados con pena de prisión de dos meses a dos años y multa de 200 a 2.000 dólares, o con una de estas dos penas.

## **JURISPRUDENCIA SOBRE DELITOS INFORMÁTICOS**

### **1. PRIMERA SENTENCIA SOBRE DELITOS INFORMÁTICOS CASO ENTEL - CONCEPCIÓN-**

**CHILE.-** <sup>109</sup>

CONCEPCION, seis de diciembre de mil novecientos noventa y nueve.

VISTO:

A fojas 5 don OFS, ingeniero, domiciliado en calle PO de Ulloa No. xxx, en Concepción, deduce recurso de protección en contra de la Empresa Nacional de Telecomunicaciones S.A., Entel S.A., representada por su Gerente Zonal don Luis Vargas, ignora segundo apellido y profesión, ambos domiciliados en calle Aníbal Pinto No. 981, en Concepción.

Manifiesta que a partir del 31 de julio de 1999 apareció en la Sección Productos y Servicios de la red Internet, en la dirección <http://www.entelchile.net>, página 2, un aviso de ofrecimientos sexuales, en la que figura como remitente su hija PFA, de 17 años, estudiante de Cuarto Año Medio en el Colegio XXX, señalando como teléfono de contacto el fono XXXXXX, correspondiente a su domicilio y que tiene el carácter de privado, cuyos aberrantes términos constan en la copia impresa de la página que acompaña. Que producto del aviso miembros de su familia han recibido innumerables llamadas telefónicas obscenas, insultantes, groseras y pervertidas que los ha obligado a pedir la suspensión del servicio telefónico y que están causando

<sup>109</sup> Agradecemos al Dr. Humberto Carrasco Blanc, Director de la Revista Electrónica de Derecho Informático, el habernos proporcionado el texto íntegro de la Sentencia que transcribimos.

una grave e insostenible crisis emocional a su familia e hija, quien incluso ha debido recurrir a la ayuda de especialistas. Que en la red pública de comunicaciones vía Internet su hija figura como una prostituta.

A su juicio la actitud de la recurrida importa absoluta arbitrariedad, pues ha permitido irresponsablemente la publicación del aviso y otros de similar naturaleza por parte de personas anónimas sin verificar la identidad de sus fuentes, contribuyendo a que mentes desquiciadas utilicen el sistema atropellando la integridad física y psíquica de las personas, derecho garantizado en el No. 1 del artículo 19 de la Constitución Política de la República de Chile. La recurrida no ha ejercido debido cuidado en relación con la información que vierte a través del sistema Internet.

Expresa que la acción de Entel S.A. de poner en funcionamiento un sistema que permite la expresión de conceptos dañosos por parte de personas anónimas y la publicidad de ofrecimientos sexuales aberrantes constituye una acción arbitraria, como también lo es la omisión de no verificar la identidad de sus fuentes, dejando en la indefensión a las personas que carecen de medios para asegurar el respeto de sus derechos.

Termina solicitando se arbitren todas las medidas necesarias para restablecer el imperio del derecho y asegurar la protección de su familia, en particular de su hija, ordenando al efecto: 1) Que la recurrida elimine de modo inmediato y definitivo cualquier anuncio o publicación relacionada con los recurrentes; 2) Que se asegure, por parte de la recurrida y a favor de los recurrentes, la no inclusión de nuevos avisos sin que previamente se identifique al emisor del mismo; 3) Que se tomen todas aquellas medidas que el Tribunal estime convenientes para el adecuado resguardo de los derechos de los recurrentes.

A fojas 21 el abogado Cristian Maturana Miquel, por la recurrida Empresa Nacional de Telecomunicaciones S.A., informando el recurso formula como cuestión previa al fondo del mismo la falta de legitimación pasiva de ENTEL S.A., Expresa que la emisión de la comunicación se originó el 31 de agosto de 1999 desde el computador personal de uno de los usuarios de la página Web de Entel Chile, identificado como CGYV (xxxxxxx@entelchile.net), domiciliada en xxxxx No. xxxx, en Concepción, Que conforme a la legislación vigente, Entel tiene la calidad de Concesionario de Servicios Públicos de Comunicaciones, y en el contexto de la Ley No. 18.168, por la que se rige, se prohíbe a todos los prestatarios y permisionarios de telecomunicaciones verificar la identidad de quienes emiten mensajes, comunicaciones y, aún, controlar, censurar, interferir o intervenir en el contenido de las mismas, pudiéndose citar al respecto el artículo 36 B, letras b y c, de dicha Ley, lo que constituye una aplicación particular de la garantía del No. 5 del artículo 19 de la Constitución Política de la República de Chile. Como Entel S.A. nada tiene que ver con el origen del mensaje cuestionado, pues sólo se limitó a prestar al causante un acceso a la red virtual Internet, corresponde que el recurrente dirija la acción en contra de doña CGYV, quien aparece como legítimo contradictor con titularidad pasiva frente a su pretensión.

Expone que el servicio de acceso que presta Entel S.A. a la red Internet configura uno complementario del servicio público de telecomunicaciones conforme al artículo 8, inciso 6, de la Ley No. 18.168, reiterado en el artículo 6 del Decreto Supremo No. 425/96. Además de lo anterior, Entel S.A. facilita una página de comunicación Web, que cuenta con diversas fuentes de información y servicios tanto para usuarios y suscriptores de Entel como para cualquier persona que ingrese a ella a través de la red. uno de los servicios gratuitos corresponde a la sección denominada "Avisos clasificados" ubicada en el sitio Web <http://www.tribu.cl>, administrado por la empresa externa Grupo Web, la que a su vez tiene varias subsecciones como computación, empleos, diversión, espectáculos, etc. El sistema de avisaje es de responsabilidad de los usuarios, su publicación es muy simple y su contenido y naturaleza es clasificado por éstos. La eliminación de los avisos se realiza cada 4 a 5 días.

Explica que con posterioridad a la publicación del aviso, don RF el 04 de agosto de 1999 envió un e-mail a la casilla del administrador Grupo Web solicitando la eliminación del aviso. El 05 de agosto concurrió a las oficinas de Entel Chile en Concepción don Orlando Fuentes Siade, quien expuso al Subgerente Zonal la circunstancia que afectaba a su hija, quedando éste de solucionar el problema. Agrega que ese mismo día el administrador de la página Avisos Clasificados confirma a Entel Chile la eliminación del aviso cuestionado tras el requerimiento del padre de la persona afectada. Hace presente que la acción carece de objeto, ya que el 06 de agosto y al momento de decretarse la orden de no innovar ya no existía ningún mensaje en la red que afectara a la persona aludida o a su grupo familiar.

Señala que su representada no ha cometido acción y omisión arbitraria o ilegal alguna relacionada con las circunstancias de hecho referidas en el recurso, velando siempre por la estricta observancia del ordenamiento jurídico vigente y enmarcando su accionar a los procedimientos técnicos y reglamentarios usuales y ordinarios para esta clase de situaciones.

Solicita no se dé lugar al recurso de protección interpuesto por don Orlando Fuentes Siade por carecer de fundamentos y no existir actos y omisiones ilegales o arbitrarias imputables a Entel Chile, en los hechos en que se basa el recurso, con costas.

A fojas 41 corre informe de la Subsecretaría de Telecomunicaciones en el cual se señala que el aviso dubitado fue suprimido el 05 de agosto de 1999 debido a los reclamos efectuados los días 01 y 04 de agosto por JP y R F. Igualmente indica que el sistema computacional que soporta el funcionamiento de la página web permite fácilmente borrar los avisos. Acompaña los documentos de fojas 36 a 40.

A fojas 43, 46 y 81 el abogado de la recurrida, don Javier Zehnder Gillibrand, amplía el informe de fojas 21 al tenor de lo solicitado por esta Corte a fojas 33 y 35, relacionado con información y antecedentes del sitio Web Entel y el sitio web "La Tribu".

A fojas 96 rola informe del Director del Departamento de Ciencias de la Computación de la Facultad de Ciencias Físicas y Matemáticas de la Universidad de Chile. Acompaña los documentos de fojas 98 a 108.

El recurrente acompañó los documentos de fojas 1 a 4 y la recurrida los que rolan de fojas 18 a 20 y de fojas 50 a 80.

A fojas 109 se cumplieron las diligencias ordenadas para un mejor acierto del fallo.

#### **CON LO RELACIONADO Y CONSIDERANDO:**

##### **1. EN CUANTO A LA FALTA DE LEGITIMACION PASIVA DE ENTEL S.A.**

1° Que la legitimación procesal es la facultad de poder actuar en el proceso como actor, como demandado o como tercero, o representando a éstos.

Que por legitimación para obrar entiéndese la identidad de la persona del actor como la persona a la cual la ley concede la acción (legitimación activa) y la identidad de la persona del demandado con la persona contra la cual es concedida la acción (legitimación pasiva).

2° Que en la acción de protección el sujeto pasivo es la Corte de Apelaciones respectiva, por cuanto se encuentra obligada a dar protección al afectado velar por el respeto de las garantías constitucionales garantizadas y adoptar "de inmediato las providencias que juzgue necesarias para restablecer el imperio del derecho y asegurar la debida protección del afectado".

"El sujeto pasivo de la acción de protección es la Corte de Apelaciones, tribunal que por mandato de la Constitución debe dar la debida protección al ofendido". "De este modo, a quien se trata de poner en la obligación de dar, hacer o hacer algo es a la Corte de Apelaciones respectiva, la que por ello pasa a ser sujeto pasivo de la acción" (ERRÁZURIZ GATICA, Juan Manuel y OTERO ALVARADO, Jorge Miguel, Aspectos Procesales del Recurso de Protección, Edit. Jurídica de Chile, 1989, página 24).

3° Que la persona o personas acusantes del acto y omisión arbitraria o ilegal reclamando no tiene la calidad de sujeto pasivo de la acción, toda vez que su actuación se limita a informar, a petición de la Corte de Apelaciones, al tenor de la acción deducida por el recurrente y enviar todos los antecedentes "que existan en su poder sobre el asunto motivo del recurso".

El causante del acto y omisión arbitraria o ilegal tiene la calidad de informante, y no es parte natural de la acción. Sin embargo, conforme al No. 4 del Auto Acordado de la Excm. Corte Suprema sobre Tramitación del Recurso de Protección de Garantías Constitucionales, "las personas, funcionarios y Órganos del Estado afectados o recurridos, podrán hacerse parte en el recurso".

Que, así las cosas, se rechazará la alegación de falta de legitimación pasiva alegada por Entel S.A., por no tener ésta la calidad de "sujeto pasivo" de la acción de protección.

## II. EN CUANTO AL FONDO

4° Que la acción de protección consagrada en el artículo 20 de la Constitución Política de la República de Chile presupone la existencia de actos y omisiones, con carácter de arbitrarios o ilegales, que realmente priven, perturben o amenacen el debido ejercicio de los derechos tutelados, teniendo como objetivo básico reaccionar prontamente contra situaciones de hecho, evidentemente anormales, que lesionan alguna garantía individual determinada, o sea restablecer el derecho alterado ilegalmente, y mantener y restablecer el status que existente en cuanto a los derechos de las partes con anterioridad a los actos u omisiones perturbatorias.

5° Que el recurrente hace consistir el acto y omisión arbitrario o ilegal en el hecho que a contar del 31 de julio de 1999 apareció en la sección Productos y Servicios de la red Internet en la dirección <http://www.entelchile.net/> un aviso de ofrecimientos sexuales aberrantes, en que figuraba como remitente su hija PFA, de 17 años de edad, estudiante, y en el que se indicaba como teléfono de contacto su fono privado, recibándose en su hogar innumerables llamadas obscenas, insultantes, groseras y pervertidas, por lo que tuvo que suspender el servicio telefónico. Considera que Entel S.A. ha puesto en funcionamiento un sistema que permite la indiscriminada expresión de conceptos dañinos por personas anónimas y la publicación de avisos como el señalado y de otros más de similar naturaleza, sin verificar la identidad de quien aparece como emisor de la publicación. No tiene, por tanto, el debido cuidado en relación a la información que vierte a través del sistema Internet, contribuyendo así a que mentes desquiciadas usen el sistema para destruir la vida, el honor, la dignidad y la integridad moral de personas inocentes e indefensas, como es el caso de su hija menor de edad, que figura en la red pública de comunicaciones vía Internet como una prostituta.

El recurrente solicita que la recurrida elimine de modo inmediato y definitivo cualquier anuncio o publicación relacionada con su familia, que asegure por parte de la recurrida y a su favor la no inclusión de nuevos avisos sin que, previamente, se identifique al emisor del mismo y que se tomen todas las medidas convenientes para el adecuado resguardo de los derechos de los recurrentes.

6° Que el recurrente con los documentos acompañados a fojas 1 a 4 ha acreditado que el día 31 de julio de 1999, a las 21:05, apareció en el sitio Web la Tribu dentro de la página Web de Entel, un aviso cuyo contenido es del tenor siguiente:  
"Me ofrezco para todo tipo de servicios masculinos (bailes 1000 pesos/hora), masajes, posiciones exóticas, sexo a la carta (oral, anal, legal, etc). gays y lesbianas bienvenidos. Concepción fono xxxxx. Discreción asegurada. LLAMAME!!!  
PFA -xxxxxxx@hotmail.com

Saturday 31 jul 1999 at 21:=5"

7° Que informando el representante de la recurrida ENTEL S.A. señala que ésta tiene la calidad de concesionaria de servicios públicos de Telecomunicaciones, suministrando como servicio complementario de telecomunicaciones uno de acceso a la red mundial Internet. Además facilita una página de comunicación Web, que cuenta con diversas fuentes de información y servicios tanto para usuarios y suscriptores de Entel, como para cualquier persona que ingresa a ella a través de la red, figurando entre los servicios gratuitos una sección denominada "Avisos Clasificados" ubicada en el sitio Web <http://www.tribu.cl>), sección que consta de varias

subsecciones agrupadas de acuerdo al rubro de aviso, entre ellas "Empleo" y "Diversión, espectáculos", la que es administrada por la empresa "Grupoweb".

Indica que el aviso cuestionado fue publicado en el sitio Web <http://www.tribu.cl/>, sección "Avisos Clasificados", subsección "Diversión, espectáculos", emitiéndose desde el computador personal de uno de los usuarios de la página Web de Entel Chile identificado como CGYV, casilla e-mail xxxxxxx@entelchile.net.

8° Que Entel S.A. en su calidad de concesionaria de servicios públicos de telecomunicaciones se rige por la Ley No. 18.168, de 1982, sobre Ley General de Telecomunicaciones. El inciso 6° del artículo 8 de la ley citada la faculta para dar prestaciones complementarias por medio de las redes públicas, de modo que puede proveer de servicio de acceso a Internet.

El artículo 6 del Decreto Supremo No. 425, de 1996, que Aprueba el Reglamento del Servicio Público Telefónico, precisa los "*servicios complementarios*" como servicios adicionales que se suministran por medio de las redes públicas, mediante la conexión de equipos a dichas redes.

A su vez, en la resolución No 1483, de 1999, de la Subsecretaría de Telecomunicaciones se define el "Servicio de Acceso a Internet" como el servicio que permite acceder a la información y aplicaciones disponibles en la red Internet, y el "Proveedor de Acceso a Internet, ISP" como la persona natural o jurídica que presta el servicio de acceso a Internet, de conformidad a la ley y su normativa complementaria.

9° Que consta en autos (fojas 46 y 81) que Entel S.A. tiene inscrito a su nombre el dominio <http://www.entelchile.net/> en el cual funciona la "homepage" Web Entel, cuyos sistemas de Hardware y servidores se encuentran materialmente en territorio chileno, lo mismo el servidor que sirve de plataforma al sitio <http://tribu.grupoweb.cl/>.

Igualmente consta que tiene la calidad de proveedor de alojamiento respecto del sitio web La Tribu, cuya dirección es <http://tribu.grupoweb.cl/> que es administrado por la empresa "Grupo Web", que corresponde a la persona jurídica "Roseta Perey y Compañía Limitada", siendo la empresa dueña del nombre de dominio "grupoweb.cl/" y del subdominio "tribu.grupoweb.cl".

10° Que cualquier persona puede efectuar la publicación de un aviso en el sitio Web La Tribu, servicio que es gratuito. Sin embargo, a pesar de ser el sistema de avisaje muy simple y automatizado, es necesario que el usuario conozca la clave de acceso a Internet, debe tener un "Passaporte" Tribu y un e-mail o correo electrónico, y al momento de redactar el contenido del aviso en el formulario respectivo debe consignar su nombre y su e-mail.

11° Que de los antecedentes acompañados a los cautos fluye que el administrador del sitio Web La Tribu revisa la sección "Avisos Clasificados", subsección "Empleo" y "Diversión, espectáculos", cada 3 a 5 días, o una vez a la semana, eliminando aquéllos inapropiados, las ofertas caducadas, los que se encuentran en secciones equivocadas, los que solicitan los propios interesados, y periódicamente todos aquellos que llevan más de dos meses de publicados. Sólo el administrador puede eliminar los avisos insertos en las respectivas secciones y subsecciones.

En el informe de la Subsecretaría de Telecomunicaciones de fojas 41 se indica que el sistema computacional que soporta el funcionamiento de la página Web permite fácilmente borrar cualquier aviso.

En la Tribu se iniciaron diversas gestiones ante el administrador del sitio y la recurrida, respectivamente.

El 01 de agosto de 1999, a las 10:24 horas (fojas 36 a 40), doña Javiera Puentes envió un mensaje a "sugerencias@entelchile.net" solicitando, como hija del usuario cgyanezv, que borrarán el aviso inserto en las secciones "Empleo" y "Diversión, espectáculos".

El 04 de agosto de 1999, a las 18:40:58 GMT don RF desde la casilla electrónica xxxxxxxxxxx@hotmail.com envía un mensaje a la casilla [tribu@entelchile.net](mailto:tribu@entelchile.net) pidiendo que

suprimieran el aviso por afectar a una amiga menor de edad, reiterando la solicitud el jueves 05 de agosto, a las 00:24:35 GMT.

Finalmente, el 05 de agosto de 1999, alrededor de las 15:30 horas, don Orlando Fuentes Siade concurre a las oficinas de Entel Chile en Concepción, entrevistándose con el Subgerente Zonal a quien expuso la circunstancia que afectaba a su hija, quedando éste de solucionar el problema.

13° Que en Chile no existe un marco jurídico específico sobre regulación de la red Internet.

El marco regulatorio de la Ley No. 18.168, de 1982, sobre Ley General de Telecomunicaciones, no alcanza a la red Internet que opera en el sector de las comunicaciones.

Que no obstante lo anterior, los problemas originados en la red Internet deben ser resueltos conforme a las normas contenidas en la Constitución Política de la República de Chile y a las reglas generales sobre responsabilidad civil y penal.

14° Que en nuestro país en agosto de 1999 ingresó en la Cámara de Diputados un Proyecto de Ley sobre Regulación de Internet, en el que se sostiene que "en un Estado de derecho los medios de comunicación masiva deben observar deberes y responsabilidades específicas para quienes se desempeñan en estos organismos. Esta situación, que es más obvia tratándose de los medios tradicionales, es decir, prensa escrita, radio y televisión, se alteran cuando se trata de defender los derechos en medios electrónicos como la Internet".

El proyecto de Ley señala que: "La libertad de informar tiene su límite natural en el respeto a los derechos con reconocimiento constitucional y legal y, especialmente, en el derecho al honor, a la intimidad, a la propia imagen y a la protección de la juventud y de la infancia.

"Por ello su ejercicio entraña deberes y responsabilidades, y podrá ser sometido a ciertas formalidades, condiciones, restricciones o sanciones, que constituyan medidas necesarias en una sociedad democrática, para la seguridad nacional, la integridad territorial o la seguridad pública, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, la protección de la reputación o de los derechos ajenos, para impedir la divulgación de informaciones confidenciales o para garantizar la autoridad y la imparcialidad del Poder Judicial" CÁMARA DE DIPUTADOS. CHILE. Boletín No. 2395-19.

15° Que, de todo lo expuesto, fluye que el aviso publicado en el sitio Web La Tribu vulnera los derechos y garantías constitucionales consagrados en el artículo 19 n°s 1 y 4 de la Constitución Política de la República de Chile, esto es, el derecho a la integridad física y psíquica de la persona y el derecho a la honra de la persona y de su familia. Más precisamente, atenta contra el derecho a la integridad psíquica de la menor afectada, entendido éste como el que le asegura el equilibrio mental y espiritual de su ser, toda vez que, como consecuencia de la publicación del aviso, recibió en su hogar numerosas llamadas telefónicas "obscenas, insultantes, groseras y perversas" que alteraron su estado mental y espiritual. Asimismo, vulnera su derecho a la honra, comprendido éste como el que le asegura el buen nombre, prestigio, honor, reputación o buena fama, y la "honra" como la buena opinión y fama adquirida por la virtud y el mérito, por cuanto, conforme al aviso, ésta aparece ante su entorno social como una persona dedicada a actividades sexuales anormales.

16° Que la recurrida ha informado a fojas 29, 47 y 89 que el aviso fue eliminado de la página "Avisos Clasificados" el 05 de agosto de 1999, siendo las 10:11 PM.

La información indicada se encuentra corroborada por los documentos acompañados de fojas 36 a 40 y por el informe de la Subsecretaría de Telecomunicaciones de fojas 41, en el cual se señala que el aviso fue suprimido el 05 de agosto de 1999, no pudiendo determinarse, según ésta, la hora en que se efectuó tal operación.

17° Que la "red" es cualquier sistema que conecta ordenadores, con el fin de permitir el acceso común a los recursos de los demás elementos que integran el sistema.

Que definiendo Internet puede decirse que es la red de redes o una colección de redes entrelazadas. Más concretamente, como una red mundial de computadores interconectada a través de oferentes oficializados o un sistema de redes de computadores que permite el intercambio de información.

Se sostiene que Internet es un "medio de comunicación" basado en la libertad para la circulación de información. En cambio, para otros sólo es un "medio de transporte de información", porque aquí fluye información de todo tipo, que no se genera en el medio, como en la radio o la televisión, sino que hay información de todo el mundo.

La red Internet se caracteriza por no tener dueño ni gerente ni representante legal, por ser de alcance mundial y de acceso general.

18° Que la conducta de las personas que participan en el "ciberespacio" puede dar origen a hechos ilícitos que deriven en responsabilidades civiles y penales.

La responsabilidad por conductas realizadas en Internet dependerá de las funciones que el "actor de Internet" o usuario de la red se encuentre realizando al momento de producirse el hecho generador de ésta.

Un usuario de la red de Internet puede, simultáneamente, desempeñar varias funciones. Normalmente las responsabilidades se radican en dos o más usuarios. No obstante, delimitarlas y hacerlas efectivas es tarea de suyo compleja.

19° Que en un sitio Web pueden publicarse y divulgarse contenidos ilícitos o nocivos, sean mensajes, avisos o bienes protegidos por propiedad intelectual que no cuenten con autorización, cuya utilización cause daño a la honra y bienes de terceros, invadiendo su vida privada e intimidad vulnerando su honra o atentando contra su patrimonio, incluso, tales avisos o mensajes pueden llegar a ser contrarios a la ley, el orden público, a la seguridad nacional o a la moral o a las buenas costumbres.

En la delimitación de las responsabilidades son actores en Internet: el proveedor de acceso a la red, el proveedor de sitio o de almacenamiento el proveedor de contenido y los usuarios o destinatarios finales del servicio.

El proveedor de acceso permite que un determinado usuario se conecte con la red Internet, que de no existir ese acceso haría imposible la comisión del ilícito; el proveedor de sitio o de almacenamiento, en la medida que permita que un determinado sitio Web en el que se cometan actos ilícitos permanezca almacenado en su propio servidor, que de no contar con este dispositivo técnico haría imposible la existencia o permanencia de ese sitio Web en Internet; y en proveedor de contenido, por ser el que directamente incorpora contenidos ilícitos bajo su tuición en un determinado sitio Web.

20° Que en la situación en estudio tiene la calidad de abonado o suscriptora doña CYV y la de usuario final ésta o la persona que publicó el aviso cuestionado.

Ahora bien, Entel S.A. tiene la calidad de proveedor de acceso y de proveedor de alojamiento respecto del sitio <http://tribu.grupoweb.cl/>.

Finalmente, la calidad de proveedor de contenido la tiene la empresa "Grupoweb".

21° Que en opinión del profesor de Propiedad Intelectual de la Facultad de Derecho de la Universidad de Chile y Director General de la Sociedad Chilena del Derecho de Autor, abogado señor Santiago Schuster Vergara, la responsabilidad recae directamente en el usuario proveedor de contenido en la red, cuando tal contenido es ilícito o nocivo, y que tal responsabilidad podría incluso extenderse a aquellos contenidos que son incorporados directamente por los destinatarios finales del servicio Internet, cuando el proveedor de sitio (en calidad de los que se llama "proveedor conjunto de contenido") ha creado un fondo de información con los aportes de los clientes de sus diferentes foros puestos a disposición de cualquier abonado a la red y no ha

tomado las providencias mínimas necesarias para la adecuada identificación de los usuarios que publican tales mensajes, a fin de asegurar las eventuales responsabilidades por el posible menoscabo a terceros.

Asimismo, sostiene el profesor Shuster Vergara que en la publicación y divulgación en un sitio Web de un aviso o mensaje con un contenido ilícito o nocivo también cabe responsabilidad al proveedor de acceso y al proveedor de alojamiento de la página Web respectiva, cuando, a sabiendas de la actividad ilícita que se realiza por los abonados a su servicio, no ha retirado los datos o no ha hecho que el acceso a ellos sea imposible, como asimismo cuando, sabiendo la actividad ilícita que se realiza por los abonados de su servicio, o habiendo podido saberla, no ha retirado los datos, no ha hecho que el acceso a ellos sea imposible o incluso ha promovido ese acceso. De igual modo, es responsable cuando el mismo realiza transmisiones de datos, con contenidos ilícitos, seleccionando el mismo a los destinatarios, seleccionando los datos o modificando los datos.

En estas situaciones se encuentran también la utilización de bienes protegidos por propiedad intelectual cuyo uso en la red no se encuentra autorizado.

Señala, además, que las razones que explican la responsabilidad de los proveedores de acceso se fundamentan en que, teniendo en cuenta la regla de la "anonimidad", en las transmisiones en Internet (corolario de las libertades de expresión y de información y del derecho a la privacidad), esos proveedores son un eslabón clave para la contención de las actividades ilícitas en las redes digitales.

En consecuencia -agrega- el proveedor de acceso es el único que "puede ofrecer la identificación de los infractores". Es el único que tiene las herramientas técnicas para evitar que continúen produciéndose perjuicios a las personas agraviadas en su honra como en sus bienes, caso particular de los bienes protegidos por su propiedad intelectual. El proveedor de acceso es definitivamente el único vínculo existente con los usuarios que cometen ilícitos. De ahí que muchas de las acciones de las personas agraviadas se dirigirán primero a ellos, para notificarles del ilícito y para exigir una acción de cesación del servicio hacia los infractores. Las mismas razones son válidas para los proveedores de sitio o alojamiento de datos, respecto de quienes instalan sitios web en sus servidores.

El profesor Schuster señala que en las infracciones que se producen en las redes digitales es evidente la responsabilidad del proveedor de servicios de alojamiento, cuando éste, conociendo su ilicitud o habiendo podido conocerla, permite que a través de los servicios que presta se cometan hechos ilícitos, puesto que mediante este comportamiento (culposo o negligente) se coloca en situación de cooperador de la ilicitud y de responsable de la misma, por la acción de mantener el servicio o por la omisión de no proceder a su cese en forma oportuna (SCHUSTER VERGARA, Santiago. Conferencia sobre "Responsabilidad Legal en las Redes Digitales", Santiago de Chile, 1999, no publicada).

22° Que en cuanto a las obligaciones que incumben al proveedor de sitio, aunque no esté personalmente en el origen de un mensaje, el Tribunal de Primera Instancia de París, con fecha 09 de junio de 1998, ha manifestado que el prestatario "tiene la obligación de velar por la buena moralidad de aquellos que alberga, para que éstos (los proveedores de contenido) respeten las reglas de deontología que rigen el WEB, y por el respeto por ellos de las leyes y reglamentos y de los derechos de terceros. El prestatario tiene la posibilidad material de verificar el contenido del sitio en el que ofrece alojamiento y de tomar, por consiguiente, si es necesario, las medidas susceptibles de hacer cesar el perjuicio que hubiera sido causado a un tercero". Tiene el deber de informar al que alberga (proveedor de contenido), de su "obligación de respetar los derechos de la personalidad, el derecho de los autores y los derechos de las marcas" (Revue Internationale Du Droit D'Auteur, enero de 1999, n°179, página 342).

El proveedor de sitio, aún cuando no esté personalmente en un mensaje, que no tiene el carácter de "correspondencia privada", que perjudica los derechos de un tercero o de la sociedad, tiene la obligación de velar por el respeto de esos derechos.

23° Que, como se dijo en los razonamientos anteriores, consta en autos que el aviso cuestionado fue suprimido de la sección "Avisos Clasificados" en el sitio web La Tribu el 05 de agosto de 1999.

El recurrente Orlando Fuentes Siade dedujo la acción de protección con fecha 06 de agosto de 1999, según consta a fojas 5, y la orden de no innovar que solicitó fue concedida con esa misma fecha (fojas 7 vuelta).

Que cabe concluir que a la fecha de interposición del recurso y de la concesión de la orden de no innovar no existía el aviso cuestionado por el recurrente.

En relación a la identidad del emisor del aviso, ésta queda determinada suficientemente, toda vez que la persona que desee publicar un aviso en el sitio web La Tribu debe consignar la clave de acceso a Internet del suscriptor, tener un "Passaporte" Tribu y un e-mail y, al redactar el aviso, indicar su nombre y su e-mail. Ahora bien, que los datos y antecedentes entregados por el usuario sean verídicos dependerá únicamente de la buena fe con que éste actúe en la red Internet.

24° Que, en consecuencia, no existiendo el 06 de agosto de 1999 ningún aviso o mensaje en la red Internet que aludiera a la hija del recurrente o a cualquier miembro de su grupo familiar y estimándose posible identificar al emisor de éstos, forzoso es concluir que a la fecha indicada no existía derecho constitucional conculcado que proteger, careciendo la acción de objetivo por haberse restablecido el statu quo vigente a los hechos denunciados, sin intervención de la justicia, por lo que la acción cautelar perdió oportunidad.

25° Que habiendo perdido oportunidad la presente acción constitucional, atendida su finalidad, sólo cabe rechazarla.

Sin perjuicio de lo anterior, la recurrida Entel S.A. en su calidad de proveedor de acceso y de alojamiento deberá adoptar todas las medidas técnicas y fácticas que sean necesarias, que no signifiquen censura, para que en lo sucesivo la empresa "Grupoweb", en su calidad de proveedor de contenido, se abstenga de publicar avisos que en el país, de conformidad con el ordenamiento jurídico vigente, sean contrarios a la Ley, el orden público o a las buenas costumbres, y proceda el Administrador de la sección "Avisos Clasificados" subsección "Empleo" y "Diversión, espectáculos" ubicada en el sitio web <http://www.tribu.cl/> a eliminar, a lo menos dos veces a la semana, todos los avisos contrarios a las normas y valores señalados precedentemente.

Por estas consideraciones y lo dispuesto en los artículos 19 y 20 de la Constitución Política de la República de Chile y en el Auto Acordado de Garantías Constitucionales; se declara que SE RECHAZA, sin costas, la acción de protección deducida en lo principal de la presentación de fojas 5 por don Orlando Fuentes Siade en contra de la Empresa Nacional de Telecomunicaciones S.A., ENTEL S.A., representada por su Gerente Zonal señor Luis Vargas París.

Regístrese, comuníquese y archívese en su oportunidad.  
Redacción del Ministro Titular señor Juan Clodomiro Villa Sanhueza

## **2.- SEGUNDA SENTENCIA RELATIVA A DELITOS INFORMÁTICOS. CASO HISPAAHACK. BARCELONA - ESPAÑA.-**

---

### **JUZGADO DE LO PENAL NÚM. DOS BARCELONA**

En Barcelona, a veintiocho de mayo de mil novecientos noventa y nueve.

El Ilmo. Sr. D JUAN CARLOS LLAVONA CALDERON, Magistrado-Juez del Juzgado de lo Penal nº 2 de los de esta capital, ha visto en juicio oral y publico las presentes actuaciones de Procedimiento Abreviado Nº 130/99-E de la Ley Orgánica 7/1988, de 28 de diciembre, dimanante de Diligencias Previas nº 1206/98 del Juzgado de Instrucción nº 20 de Barcelona, seguidas por un presunto delito de daños contra el acusado JFS en libertad provisional por esta causa, defendido por el Abogado Carlos A. Sánchez Almeida y representado por el Procurador Carlos Pons de Gironella, siendo parte acusadora el Ministerio Fiscal.

**ANTECEDENTES DE HECHO.- PRIMERO.-** Por el Juzgado de Instrucción nº 20 de Barcelona se incoaron Diligencias Previas nº 1206/98, en virtud de atestado instruido por la Unidad de Policía Judicial de la Guardia Civil, habiendo formulado el Ministerio Fiscal escrito de acusación contra JFS, por lo que se acordó la apertura del juicio oral, correspondiendo su conocimiento a este Juzgado, que incoó el Procedimiento abreviado.

**SEGUNDO.-** El acto del juicio oral se ha celebrado el pasado 26 de mayo, practicándose en el mismo las pruebas siguientes: Interrogatorio del acusado, Testifical de JBT, BVV, los agentes de la Guardia Civil titulares de los carnets nº 26.001.263 y 118.189, AMT y MFB, respectivamente, Pericial a cargo de JIG y PFG, y Documental.

**TERCERO.-** El Ministerio Fiscal en sus conclusiones definitivas estimó los hechos como constitutivos de un delito de daños, previsto y penado en el art 264-2 del Código Penal, del que era autor el acusado, sin la concurrencia de circunstancias modificativas de la responsabilidad criminal, solicitando que se le impusiera la pena de dos años de prisión y multa de dieciocho meses a razón de 1000 pesetas de cuota diaria, con responsabilidad personal subsidiaria de 270 días y costas.

**CUARTO.-** La defensa del acusado, en su escrito de conclusiones provisionales elevadas a definitivas, manifestó su disconformidad con las conclusiones del Ministerio Fiscal, solicitando su libre absolución.

**HECHOS PROBADOS.-** Así expresamente se declaran, que a las 4,16 horas del día 11 de septiembre de 1997 se produjo un acceso no autorizado a través de Internet en los ordenadores ubicados en las dependencias de la UPC, desde un ordenador situado en el campus de V., en G., de la Universidad de O. denominado "proy6.etsiig.uniovi.es", llegando a obtener los privilegios del administrador del sistema en al menos dieciséis máquinas servidoras e instalando programas "sniffers" destinados a capturar información que circula por la red del sistema, en concreto identificadores y claves de acceso de otros usuarios, enviando los datos obtenidos a través de Internet a un ordenador denominado "ftp.laredcafe.com" ubicado en el bar LRCC sito en la calle C. de P. de M., almacenandolos en el directorio denominado "jfs" correspondiente al usuario "Hispahack", sin que conste acreditado que el acusado JFS, mayor de edad y sin antecedentes penales, participase en esa entrada ilegal, obtención y transferencia de datos.

**FUNDAMENTOS DE DERECHO.- PRIMERO.-** Al abordar con mayor detenimiento las cuestiones previas planteadas por la defensa del acusado al comienzo del juicio oral, enseguida se advierte la escasa consistencia de las alegaciones en que se funda la declaración de nulidad pretendida, pues si por una parte, y con referencia a las investigaciones realizadas por los miembros de la Guardia Civil adscritos a la Unidad Central Operativa, éstas no precisaban de denuncia previa por parte de los afectados, ya que, aunque así sea con relación a determinadas figuras delictivas que pueden cometerse por medios informáticos o telemáticos, como es el caso del descubrimiento y revelación de secretos que tipifica el art 197 del vigente Código Penal, y conforme establece el art 201.1 del mismo Código, no ocurre lo mismo, sin embargo, con relación a otros delitos como es precisamente, aquél en que se centra la acusación formulada en esta causa, tipificado en el art. 264.2 del citado cuerpo legal, cuya persecución y castigo no se condiciona a la previa denuncia, siendo ésta en todo caso un requisito de procedibilidad una vez determinada la conducta punible y su calificación jurídico penal, pero no un óbice para la actuación de investigación de conductas supuestamente delictivas, al margen de su concreta calificación, que corresponde a las fuerzas y cuerpos de seguridad del Estado, por otra parte, y en lo que atañe a la pretendida vulneración del derecho fundamental a la intimidad y al secreto de las comunicaciones que corresponde al acusado. debe señalarse que las investigaciones realizadas respecto del mismo no han incidido en ninguno de esos derechos, y su identificación fue posible, según explica el atestado, después de haber recibido un mensaje de correo electrónico alertando sobre las actividades de unos supuestos "hackers" informáticos, al que se adjuntaban fotografías de varios de los integrantes de ese grupo, uno de ellos identificado con las iniciales Jfs, accediendo posteriormente a una página de información pública ubicada en un proveedor de Internet de Estados Unidos que, según la información contenida en la misma, pretendía ser la página de un grupo llamado "Hispahack", y en la que aparecía un artículo atribuido a jfs, y tras realizar diversas gestiones lograron localizar en Internet un ordenador conectado de nombre "jfs.hispahack.org" ubicado en la empresa GL de Gibraltar que, por medio de AAO, lograron averiguar que había sido dado de alta en la red por el acusado. Bien es cierto que para la identificación de otros supuestos integrantes de aquel grupo

se acudió al proveedor en España de Internet a fin de conocer su identidad mediante su dirección de correo electrónico, pero además de no ser éste el caso del aquí acusado, tampoco cabe entender que ello constituyese vulneración alguna del derecho fundamental al secreto de las comunicaciones, ya que no se tuvo acceso al contenido de ningún mensaje transmitido mediante correo electrónico y sí sólo al nombre de la persona que utilizaba la dirección correspondiente, de la misma manera que podría haberse identificado a un abonado del servicio telefónico a través de su número de abonado, no suponiendo ello violación de derecho fundamental alguno, ni siquiera de las prescripciones que para el acceso y transmisión de datos personales contiene la Ley Orgánica Reguladora del Tratamiento Automatizado de Datos de carácter personal, pues la propia Ley excluye de la necesidad del consentimiento del afectado la recopilación de datos que requiera el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias (art. 6.2), especialmente cuando la información al afectado impida o dificulte la persecución de infracciones penales o administrativas (art. 22.1), quedando en todo caso limitada la recogida y tratamiento automatizado de datos de carácter personal por las fuerzas y cuerpos de seguridad del Estado, sin el consentimiento de las personas afectadas, a aquellos supuestos y categorías de datos que resulten necesarios para la represión de infracciones penales (art. 20.2). En suma, no cabe sino reiterar aquí nuevamente el rechazo a la pretensión de nulidad de parte de las actuaciones llevadas a cabo en esta causa que plantea la defensa del acusado. Por lo demás, y en contra de lo que sostiene dicha parte, no se cuestiona aquí el ejercicio de la libertad de expresión través de Internet, sino que el enjuiciamiento se centra en una actividad que con la expresión anglosajona "hacking" (intrusismo informático) hace referencia a un conjunto de comportamientos de acceso o interferencia no autorizados a un sistema informático o red de comunicación electrónica de datos, y a la utilización de los mismos sin autorización o más allá de lo autorizado, conductas que, en cuanto suponen de agresión contra el interés del titular de un determinado sistema de que la información que en él se contiene no sea interceptada, resultan tanto más reprobables, y aún merecedoras de sanción penal si - como suele ser lo habitual - atentan contra sistemas o equipos informáticos particularmente relevantes que, por razón del contenido de la información que procesan o almacenan y por las funciones que tienen asignadas en el seno de las relaciones jurídicas, económicas y sociales, afectan gravemente a un interés supraindividual o colectivo, de manera que plantear en esta sede una adecuada tutela penal autónoma frente al intrusismo informático no puede en modo alguno considerarse un exceso de reacción penal.

**SEGUNDO.-** Los hechos que se declaran probados en esta resolución son el resultado de una apreciación en conciencia de las pruebas practicadas en el juicio, conforme a lo dispuesto por el art. 741 de la Ley de Enjuiciamiento Criminal, y así, en efecto, el informe elaborado en su momento, y ratificado en dicho acto plenario como testigo, por JBT refiere la existencia de un ataque a los sistemas informáticos de la UPC con resultado de obtención de privilegios de administrador e instalación de programas "sniffers", afectando al menos a dieciséis máquinas servidoras y haciendo uso de herramientas para capturar información en las menos cinco de ellas, concretamente identificadores y claves de acceso de otros usuarios, ataque realizado desde una máquina perteneciente a la UO y que remitió la información obtenida a otra máquina instalada en PM (folios 15 y 16). No cabe reputar acreditada, sin embargo, la autoría que de tales hechos se atribuye al acusado JFS, pues si bien existen fundadas sospechas de que pudo tener algún tipo de participación en ellos, ya que por una parte él mismo reconoce su pertenencia al grupo denominado "Hispahack" y la utilización del apodo "jfs", que corresponden al usuario y directorio, respectivamente, del ordenador instalado en el Bar "LRCC" al que se transfirieron los datos obtenidos en el sistema informático de la UPC, habiéndose comprobado además, en el examen del disco duro de los ordenadores que tenía en su domicilio de Martorell, intervenidos en la diligencia de entrada y registro practicada en el mismo, según expresa el perito JIG, la presencia de programas para aprovechar las vulnerabilidades de otros sistemas, ficheros de claves cifradas de usuarios de servidores y resultados de "sniffers" que incluyen identificadores de usuarios y llaves de acceso a máquinas de la UB y a la UO, sin embargo tales sospechas no alcanzan la categoría de indicios bastantes como para desvirtuar totalmente la presunción de inocencia en cuanto a la concreta participación que en esos hechos se le atribuye, pues si por una parte el acceso al ordenador de PM, y a través de él al directorio "jfs", se hallaba al alcance de cualquiera que lo hiciese a través de usuario "Hispahack", en el que el mismo perito, al examinar el disco de dicho ordenador también intervenido tras la diligencia de entrada y registro practicada en el local donde se hallaba instalado, ha comprobado la existencia de ficheros de datos y utilidades relacionadas con los problemas de seguridad de los sistemas Unix, conteniendo información sobre vulnerabilidades de máquinas, programas para explotar fallos de seguridad, "sniffers" y otras utilidades conocidas como "utilidades de hacking", al alcance de cualquiera que pudiera acceder a

dicho ordenador como usuario "Hispahack", ni el informe de FOF sobre el ordenador de la Universidad de Oviedo, a través del cual se accedió a los sistemas de la UPC, ha podido definir el origen de la intrusión no permitida a través de Internet, constatando la existencia de un directorio compartido accesible a cualquier máquina, sin claves, montado por otras dos máquinas desconocidas, ni el examen de los ficheros contenidos en los discos instalados en los ordenadores del acusado ha permitido establecer que éste poseyese información de aquellos sistemas. Ya el propio testigo JBT admite que posiblemente la persona que usaba los "sniffers" era la misma persona que los instaló, pero no puede afirmarlo con certeza, el perito JIG afirma que los ficheros con códigos de usuarios y llaves de paso detectados en las máquinas del acusado fueron generados por "sniffers" que alguien (sin precisar quién) instaló en servidores de diferentes organizaciones, y conviene con el también perito PFG en que entre tales ficheros no se hallaba ninguno de password de la UPC. No apareciendo acreditado, por tanto, más allá de toda duda razonable, que fuese el acusado quien alteró los programas contenidos en el sistema informático de dicha Universidad haciendo necesaria su total reinstalación, que es la conducta sancionada penalmente que se le atribuye, no cabe llegar a otro pronunciamiento que el de su libre absolución.

**TERCERO.-** Procede declarar de oficio las costas ocasionadas de conformidad con lo establecido por los arts. 239 y 240.1º de la Ley de Enjuiciamiento Criminal

Vistos los preceptos legales citados y demás de general y pertinente aplicación,

**F A L L O.-** Que debo de absolver y absuelvo libremente a JFS del delito de daños de que venía siendo acusado en este procedimiento, declarando de oficio las costas ocasionadas.

Líbrese y únase certificación de esta resolución a las actuaciones, con inclusión de la original en el Libro de Sentencias.

Así por esta mi sentencia, definitivamente juzgando, lo pronuncio mando y firmo.

# GLOSARIO DE TÉRMINOS

## **BAND WIDTH**

---

Ancho de banda. Se refiere a la velocidad de transmisión o a la cantidad de información que se puede transmitir por segundo. Por lo general se mide en Bytes por segundo o Kb por segundo (Kbps).

## **BANNER**

---

Es la forma que toma la publicidad en la *Web*. Es un gráfico o un logo que contiene un mensaje promocional de la empresa que lo pone. Por lo general miden entre 5 y 10 cm. de largo por 2 de ancho. El usuario que se siente atraído por el mensaje, puede *clickear* sobre él y dirigirse a la pagina donde la empresa tiene mas información.

## **BOOKMARK**

---

Es un libro de direcciones de páginas *web*. Se pueden catalogar por tema, así, a medida que uno navega, puede ir dejando anotadas las direcciones de los *sites* que más le interesaron para poder volver a visitarlas mas adelante. Evita anotar direcciones en un papel.

## **BROWSER**

---

Software que se utiliza para poder navegar en la WWW. Es el "visor" que se utiliza para poder acceder a la información publicada en la Web. Los browsers más populares son el Netscape Communicator y el Microsoft Explorer.

## **BIT**

---

Es la mínima unidad de almacenamiento de información. Un bit puede tener el valor 0 ó 1. Por este motivo la informática utiliza los códigos binarios (base 2).

## **BYTE**

---

Es el equivalente a 8 bits. Forma una carácter de información. Así, una letra como "r" o un número como el "2" o un símbolo como "@" representan un byte. El Kilobyte (Kb) son 1.024 bytes ( $2^{10}$ ). El Megabyte (Mb) son 1.024 Kb. El Gigabyte (Gb) son 1.024 Mb.

## **CIBERESPACIO**

---

Término utilizado para describir un mundo de computadores conectadas en red, acuñado por William Gibson en su libro "Neuromante". Es un mundo virtual "no real" que tiene vida propia.

## **CLICK**

---

Apretar el botón del mouse sobre algún elemento de la página.

## **COOKIE**

---

Es un archivo que guarda el *browser* del usuario que contiene información acerca de él. Según la información que el usuario les brinda a los distintos *web sites*, muchos de éstos accesan a esa información directamente cuando se regresa a esa página, sin necesidad de volver a ingresar información nuevamente o acatando la configuración del *web site* que se eligió previamente.

## **DOWNLOAD**

---

Descargar. Quiere decir bajar (copiar) archivos desde una computadora remota a la suya.

## **E-MAIL**

---

Conocido como correo electrónico. Es una de las herramientas más efectivas que ofrece la red. Permite intercambiar mensajes electrónicamente con otros usuarios sin importar en qué parte del mundo se encuentren. Es similar al correo tradicional (tiene un destinatario, un tema y un desarrollo) pero solamente es distribuido en forma electrónica en cuestión de segundos.

## **EXTRANET**

---

Se refiere a la red interconectada de Intranets entre un fabricante y su proveedor o de un fabricante con sus distribuidores. La mayor parte de los recursos se comparten pero existen limitaciones de acceso.

## **FAQ**

---

Frequently Asked Questions. Preguntas que se hacen más frecuentemente. Documento o página web que contiene las preguntas y respuestas más comúnmente usadas sobre un mismo tema.

## **FILE TRANSFER PROTOCOL**

---

También llamado FTP, es una de las aplicaciones de Internet para transferencias de archivos. Mediante un directorio, seleccionamos el documento o archivo buscado y "trasladamos" el mismo hasta nuestro computador. Algunas páginas de la WWW que ofrecen archivos, direccionan mediante un link a una servidor FTP para copiar la información. Existen FTPs anónimos o de acceso público y privados, que requieren de una contraseña para el acceso.

## **GIF**

---

Formato de gráficos utilizado en la WWW. También existe el formato JPG.

## **GATEWAY**

---

Puerta de Salida. Es el proveedor o la empresa que provee el acceso satelital (o físico) para la entrada o salida de un grupo de usuarios o clientes al Internet.

## **HARDWARE**

---

Se refiere a toda la parte física de un equipo de computación.

## **HOME PAGE**

---

Página de acceso a un Web Site. Es la página de bienvenida y de orientación para acceder al resto de la información contenida en ese site. Es el índice de lo que contiene ese site.

## **HOST**

---

Es un server (servidor). Computadora que ofrece información para consulta por los usuarios de la Internet.

## **HTML**

---

Hypertext Markup Language. Lenguaje de marcado de hypertextos creado para simplificar la escritura de documentos estándar. Es utilizado para construir los documentos o sites de la WWW.

## **INTERNET**

---

Red mundial de computadoras interconectadas entre si por satélites, cables de fibra óptica y por vía telefónica.

## **INTRANET**

---

Red de computadoras "internas" o pertenecientes a una misma oficina u organización. Por lo general están conectadas entre si y tienen acceso al Internet.

## **IRC O CHAT**

---

Servicio de Internet que permite mantener una "conversación" en tiempo real entre varios usuarios de la red, usando un interface de texto.

## **ISP**

---

Internet Service Provider. Proveedor de servicios de Internet. Es la empresa u organización que ofrece servicio de Internet al público, ya sea mediante cuentas personales de Dial Up o líneas dedicadas.

## **JAVA**

---

Lenguaje de programación desarrollado por Sun Microsystems para desarrollo de aplicaciones a ser utilizadas en la red. Es una variante del lenguaje de programación C.

## **LAN**

---

Local Area Network. Red de área local. Se usa para definir una red ubicada en una misma oficina o edificio.

## **LINK**

---

Vínculo de información entre dos Web sites o dos páginas dentro del mismo site. Se utiliza para continuar la lectura o para el proceso de buscar más información. Con solo apretar el botón del mouse se puede trasladar virtualmente a cualquier otra computadora.

## **MACINTOSH**

---

Marca de computadores desarrollada por Apple Computer Inc. Es el segundo formato de computador más utilizado después del IBM compatible o PC.

## **MODEM**

---

Significa modulador – demodulador. Es el aparato electrónico (puede ser también una tarjeta interna) que le permite al computador transmitir o recibir información a través de la línea telefónica.

## **MPG**

---

Formato de archivos de video.

## **NAVEGAR**

---

Saltar de página en página dentro de la red. Se aprovecha la característica hipertexto y de vínculos (links)

## **PPP**

---

Point to Point Protocol. Protocolo de comunicaciones punto a punto para acceso de un computador con un servidor de Internet.

## **POWER PC**

---

Serie de computadores de Apple que combinan un chip Intel capaz de trabajar con archivos Mac y PC.

## **REAL AUDIO**

---

Formato comercial para transmisión de audio en tiempo real a través de la WWW. Del mismo fabricante existe el formato REAL VIDEO.

## **REALIDAD VIRTUAL**

---

Simulación basada en gráficos tridimensionales, donde el usuario puede moverse e interactuar con el ambiente simulado.

## **RUTEADOR**

---

Router. Dispositivo que direcciona información entre dos redes usando el mismo conjunto de protocolos.

## **SERVER**

---

Servidor. Computador que funciona como Host para Internet y como referencia y vínculo principal en una Intranet. Es el computador principal que direcciona la información.

## **SITE**

---

Sitio. Es el conjunto coherente y unificado de páginas y objetos intercomunicados alojados en un server. En lenguaje coloquial se utiliza este término para referirse a un lugar de la red.

## **SOFTWARE**

---

Es toda la parte lógica de un sistema de computación. Son los programas que corren en un computador.

## **TCP/IP**

---

Transmission Control Protocol / Internet Protocol. Protocolo de control de transmisión, protocolo de Internet. Es un conjunto de unos cien programas de comunicación de datos usados para organizar las computadoras en redes.

## **URL**

---

Uniform Resource Locator. Localizador uniforme de recursos. Es la dirección electrónica de un site en Internet. Es lo que debemos introducir al computador para acceder a ese sitio.

## **WAN**

---

Wide Area Network. Red de área amplia. Se utiliza para designar redes con computadores geográficamente dispersos en otros países u otras ciudades.

## **WEB SITE**

---

Comúnmente conocido como SITE. Lugar en Internet compuesto por un conjunto de páginas que informan a los usuarios acerca de lo que la empresa desea comunicarles.

## **WINDOWS**

---

Sistema operativo de Microsoft utilizado en aproximadamente el 90% de las computadoras personales. La versión mas utilizada actualmente es Windows 95. La versión 98 se está popularizando y Windows 2000 o Windows NT 5.0 tiene apenas unos meses en mercado.

## **WORLD WIDE WEB**

---

También llamada WWW o Web. Es la aplicación multimedia de Internet. Permite trabajar con gráficos, sonido, texto, audio, video, etc.

## **CONCLUSIONES**

- 1.- Entre la Ciencia del Derecho y las Ciencias Informáticas y de las Nuevas Tecnologías existen varias relaciones. Si aplicamos las Tecnologías Informáticas con el objetivo de adoptar herramientas de solución a los quehaceres en el mundo jurídico nos encontraremos frente a la Informática Jurídica. Si, en cambio analizamos las normas legales que se encaminan a la regulación de las Nuevas Tecnologías de la Información y de la comunicación, llegaremos al campo del Derecho Informático.
- 2.- La intimidad forma parte de los derechos de la personalidad que no han surgido como consecuencia del impacto de las Ciencias Informáticas en la sociedad, sino que han sido llevados a un primer plano debido a la injerencia de éstas últimas.
- 3.- Hay la necesidad de equilibrar dos intereses jurídicos en conflicto; por un lado, el derecho a controlar la propia información, y, por otro, el principio de la libertad de dar y recibir información.
- 4.- Es necesario conceptualizar al delito informático como una conducta típica, antijurídica y culpable, en el que se utiliza la tecnología desarrollada por las Ciencias Informáticas y de las Nuevas Tecnologías o se afecta a la información contenida en un sistema de tratamiento automatizado de la misma.
- 5.- Los delitos informáticos tienen un carácter pluriofensivo. Por esta circunstancia, su comisión, en muchas ocasiones, no solo se ataca a un solo bien jurídico, sino una diversidad de ellos.
- 6.- La falta de denuncia y publicidad de los denominados delitos informáticos solo benefician al delincuente, el que seguirá actuando con total impunidad en la República del Ecuador si no se establecen normas penales que castiguen éstos ilícitos.
- 7.- Todos los comentarios y opiniones expuestas en esta investigación han tenido como fundamento la doctrina y legislación de otros estados del mundo, debido a la escasa doctrina nacional sobre el tema que motivó esta investigación.
- 8.- Este trabajo de investigación trata de aportar al conocimiento de la sociedad ecuatoriana con un estudio inicial acerca de los conceptos, definiciones, clasificaciones, normativa legal internacional y jurisprudencia relacionada con los delitos informáticos.

## **RECOMENDACIONES**

- 1.- Con la finalidad de estudiar de manera profunda al fenómeno producido por irrupción de las Ciencias Informáticas y de las Nuevas Tecnologías en la sociedad de comienzos del Siglo XXI, es necesario e imprescindible que las Universidades, Escuelas Politécnicas e Institutos Superiores de la República del Ecuador incorporen en sus programas de estudios cátedras que estudien el fenómeno de la Informática y el conjunto de normas legales que deberán regularizarla.
- 2.- Sugerimos la posibilidad de que las Facultades de Jurisprudencia del país, además de incorporar en sus programas de estudios cátedras como: Derecho Informático, Informática Jurídica, puedan crear o fundar Institutos de Investigaciones relativos a las Ciencias Informáticas y la Ciencia Jurídica, con el objetivo primordial de profundizar el estudio del fenómeno informático y su impacto en el campo del Derecho y de esta forma proponer proyectos de ley, asesorar a empresas públicas y privadas.

- 3.- Nuestros Centros de Educación Superior no deben quedar a la zaga en el estudio de la temática referente a las diversas relaciones sociales que se evidencian por la utilización de las Ciencias Informáticas y de las Nuevas Tecnologías, por ello se sugiere la realización de Seminarios, Paneles y Mesas Redondas que incluyan las Ciencias Informáticas y las Ciencias penales.
- 4.- En necesario que se establezca la tutela de la intimidad de los ciudadanos por medio de proyectos de Ley de Protección de Datos Personales.
- 5.- El Código Penal ecuatoriano merece una reforma ya que se encuentra desactualizado en la protección de necesidades humanas que requieren tutela penal por la injerencia de las Ciencias de la Informática y de las Nuevas Tecnologías.
- 6.- La tipificación de normas penales que establezcan los delitos informáticos es urgente, debido a que varias de las conductas de seres humanos se hallan en la impunidad.
- 7.- Sugerimos que la Fuerza Pública, el Ministerio Fiscal y la Función Judicial deben adoptar medidas urgentes tendientes a contar con elementos técnicos indispensables para poder investigar con éxito un delito informático.
- 8.- Sugerimos a la Policía Nacional, la creación de una división especial que investigue los ilícitos informáticos.

## **1.-BIBLIOGRAFÍA PRINCIPAL.-**

- 1.- ALVAREZ CORREA, Eduardo., *“Contratos bancarios”* Ed.Uniandes, Bogotá, 1991.
- 2.- ANDRADE SANTANDER, Diana., *“El derecho a la intimidad ”* Quito, Ecuador, 1983.
- 3.- BATTO N. Hilda, CZAR DE ZALDUENDO César., *“Derecho informático”* Felix, Ed. Depalma, 1994.
- 4.- BUSCH, Richard., *“Modernas transformaciones en la teoría del delito”* Ed.Temis, Bogotá, Colombia.
- 5.- DAVARRA RODRIGUEZ, Miguel Angel., *“Manual de Derecho Informático”*, Ed. Aranzadi, Pamplona, 1997.
- 6.- DEL PONK., Luis Marco y NADELSTICHER Mitrana., *“ Delitos de cuello blanco y reacción social ”*, Ed. Intituto de Ciencias Penales, México,1981.
- 7.- DELPIAZZO., Carlos E., y otros., *“ Introducción a la informática jurídica y al derecho informático”*, Ed.Amalio Fernández, Montevideo, 1984.
- 8.- FALCONÍ PEREZ, Miguel, *“Protección jurídica a los programas de computación ”*, Editorial EDINO, Guayaquil, Ecuador, 1991.
- 9.- FERREIRA RUBIO, Delia Matilde., *“El derecho a la intimidad”* Editorial Universitaria Buenos Aires, Argentina, 1983.
- 10.- FRÍAS CABALLERO, Jorge., y otros., *“ Teoría del delito”* Ed. Codino, Caracas, Venezuela .
- 11.- FROSINI, Vittorio., *“ Informática y Derecho ”*, Editorial TEMIS, Bogotá , Colombia, 1988.
- 12.- HANCE, Oliver., *“Leyes y Negocios en Internet. México.”* , Ed.Mc Graw Hill

Sociedad Internet, México, 1996.

**13.-** GARCÍA VALDÉS, Carlos., “ *Teoría de la pena*”, Colección Ciencias Jurídicas, Madrid, España, 1969.

**14.-** GUERRERO MATHEUS, María Fernanda y SANTOS MERA, Jaime Eduardo.,

“*Fraude informático en la banca, aspectos criminológicos*”, Ed. Jesma, Bogotá, Colombia, 1993.

**15.-** GUERRERO MATHEUS, María Fernanda., y SANTOS MERA, Jaime Eduardo, y otros., “Penalización de la criminalidad informática”, Ed. Gustavo Ibañez, Bogotá, Colombia, 1998.

**16.-** GUIBOURG, Ricardo., ALLENDE, Jorge., CAMPANELLA, Elena., “ *Manual de informática jurídica* ” Editorial ASTREA, Buenos Aires, Argentina, 1996.

**17.-** GUSTAVINO, Elías., “ *Responsabilidad Civil y otros problemas jurídicos de la computación*”, Editorial La Rocca, Buenos Aires, Argentina, 1987.

**18.-** JIJENA LEIVA, Renato Javier., “ *Chile, La protección penal de la intimidad y el delito informático*”, Editorial Jurídica de Chile, 1992.

**19.-** LEVIN, Richard B., “ *Virus informáticos por computador, tipos, protección, diagnosis*” Mc. Graw Hill, España, 1991.

**20.-**MAGLIONA MARKOVICTH, Claudio., LÓPEZ MENDEL, Macarena., “ *Delincuencia y fraude informático*”, Editorial Jurídica de Chile, 1999.

**21.-** MIR PUIG, Santiago., “ *Delincuencia Informática*”, Promociones y Publicaciones Universitarias, Barcelona, 1992.

**22.-** OCAMPO DUQUE, Marcela., y HERNANDEZ SALAME, Boris Darío, “*Derecho e informática*”, Ed. Universidad Javeriana, Bogotá, Colombia, 987.

**23.-** PACHECO KLEIN, Jorge., “*Introducción a los delitos informáticos en el ciberespacio*” Ed. Nueva Jurídica, 1998.

**24.-** PEÑA CASTRILLÓN, Gilberto., “ *Informática, Derecho Bancario y Derecho a la Intimidad*”, Fundación Jurídica Colombiana, Bogotá, 1984.

**25.-** PEÑA CASTRILLÓN, Gilberto., “ *Aspectos jurídicos de la automatización bancaria y de la confidencialidad y seguridad de sus datos*”, Ed. Kelly, Bogotá, 1979.

**26.-** QUIÑONEZ GOMEZ, Gregorio., “*Cibernética Penal: El delito computalizado*”, Ed.Epson, Venezuela, 1990.

**27.-** SEIBER, Ulrich., “ *Documentación para una aproximación al delito informático*”, Ed. PPU, Barcelona, España, 1992.

**28.-** SEIBER, Ulrich., “ *The International Handbook on Computer Crime*”, Ed. John Wiley & sons Ltd., Great Britain, 1986.

**29.-** TELLEZ VALDES, Julio., “*Derecho Informático*” 2da.ed., Ed. Mc Graw Hill, México,1996.

**30.-** VELA TREVIÑO, Sergio., “*Culpabilidad e inculpabilidad*”, México, México,

1976

**31.-** ZAVALA, Antelmo., “*El impacto social de la informática jurídico en México*” Ed. UNAM, MÉXICO, 1996.

## **2.-BIBLIOGRAFIA COMPLEMENTARIA**

- 1.- AVILES CARCELER, Ricardo., *"Delitos e ilícitos en Internet"*  
<http://www.pangea.org/inetcat/prog/P15D/index.htm>
- 2.- CÓDIGO PENAL ECUATORIANO., Corporación de Estudios y Publicaciones, Quito, Ecuador, 1999.
- 3.- CÓDIGO PENAL ESPAÑOL., <http://www.onnes.es>
- 4.- CÓDIGO SANCHEZ DE BUSTAMENTE, Leyes del Ecuador, Quito, Ecuador, 1960.
- 5.- CALLEGARI, Lidia., *"Delitos Informáticos y Legislación"* en Revista de la Facultad de Derecho y Ciencias Políticas de la Universidad Pontificia Bolivariana. Medellín, Colombia, No.70 julio-agosto y septiembre, 1985.
- 6.- CONTENIDOS ILÍCITOS Y NOCIVOS DEL INTERNET. Comunicación de la Comisión del Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones.. Bruselas, 16.10.1996 COM (96) 607.
- 7.- Computer Crime Squad " <http://www.tscm.com/compccrim>"
- 8.- DURRIER, Roberto., "Asuntos penales acerca de la tarjeta de crédito", Revista del Colegio de Abogados de Buenos Aires, T.XLIV, 1984
- 9.- FEDERAL BUREAU INVESTIGATION, *"Director's Spechees"*  
<http://www.fbi.gov/pressrm/dirspeech/dirspeech00.htm>
- 10.- GÓMEZ PEREZ, María., *"Criminalidad informática"* en Revista Electrónica de Derecho Informático, número 10. Mayo de 1999.
- 11.- NACIONES UNIDAS. Octavo Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente. La Habana. 27 de agosto a 7 de septiembre de 1990. (A/CONF.144/28/Rev.1) Nueva York, Naciones Unidas, 1991.
- 12.- PALAZZI, Pablo Andrés., " Virus Informáticos y Responsabilidad Penal", sección doctrina del diario La Ley, 16 de diciembre de 1992.
- 13.- PARLAMENTO EUROPEO, *" Directiva 97/66/CE, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones"*, 15 de diciembre de 1997., en <http://www.onnet.es/ley>.
- 14.- SANCHEZ ALMEIDA, Carlos., *" El hacking ante el Derecho Penal. Una visión libertaria"*. Revista Electrónica de Derecho Informático, número 13. Agosto de 1999.
- 15.- SIMÓN, Julio A., *" Tarjetas de crédito"*, Ed. Abeledo-Perrot, Buenos Aires, 1987.
- 16.- VEIGA, María José., *"Delitos Informáticos"* en Revista Electrónica de Derecho Informático, número 9. Abril de 1999.