UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES

LOS CONFLICTOS DE JURISDICCIÓN QUE SE SUSCITAN EN LOS DELITOS INFORMÁTICOS Y LA IMPORTANCIA DE QUE ENTRE EN VIGENCIA LA LEY DE DELITOS INFORMÁTICOS

GUILLERMO AGUSTÍN LÓPEZ

GUATEMALA, AGOSTO DE 2011

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES

LOS CONFLICTOS DE JURISDICCIÓN QUE SE SUSCITAN EN LOS DELITOS INFORMÁTICOS Y LA IMPORTANCIA DE QUE ENTRE EN VIGENCIA LA LEY DE DELITOS INFORMÁTICOS

TESIS

Presentada a la Honorable Junta Directiva

de la

Facultad de Ciencias Jurídicas y Sociales

de la

Universidad de San Carlos de Guatemala

Por

GUILLERMO AGUSTÍN LÓPEZ

Previo a conferírsele el grado académico de

LICENCIADO EN CIENCIAS JURÍDICAS Y SOCIALES

Guatemala, agosto de 2011

HONORABLE JUNTA DIRECTIVA

DE LA

FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES

DE LA

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

DECANO:	Lic. Bonerge Amilcar Mejía Orellana
VOCAL I:	Lic. César Landelino Franco López
VOCAL II:	Lic. Mario Ismael Aguilar Elizardi
VOCAL III:	Lic. Luis Fernando López Díaz
VOCAL IV:	Br. Mario Estuardo León Alegría
VOCAL V:	Br. Pablo José Calderón Gálvez
SECRETARIO:	Lic. Avidán Ortiz Orellana

RAZÓN: "Únicamente el autor es responsable de las doctrinas sustentadas y contenido de la tesis". (Artículo 43 del Normativo para la Elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Público).

Lic. ERICK ROLANDO HUITZ ENRÍQUEZ
ABOGADO Y NOTARIO
8ª. Av. 20-22 Zona 1 Oficina 8
Teléfono: 46260802

FACULTAD DE CIENCIAS JURIDICAS Y SOCIALES
UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
SECRETARIA
Guatemala, C. A.

FACULTAD DE CIENCIAS
JURIDICAS Y SOCIALES
RECIBIDO
12 ABR 2010
UNIDAD DE ASESORIA DE TESIS
Hora:
Firma:

Guatemala, 12 de abril del 2010

SEÑOR JEFE
DE LA UNIDAD DE ASESORÍA DE TESIS
DE LA FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES
DE LA UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
LICENCIADO ROLANDO SEGURA GRAJEDA
SU DESPACHO

Estimado Licenciado Segura Grajeda:

En atención a la providencia de ASESOR de tesis, de fecha diez de marzo del dos mil diez, en la que se me notifica el nombramiento como ASESOR de Tesis del Bachiller GUILLERMO AGUSTÍN LÓPEZ, y oportunamente a proceder a emitir el dictamen correspondiente. Habiendo cumplido con ASESORAR el trabajo confiado, me permito emitir el siguiente:

DICTAMEN

1) El trabajo de tesis se intitula "LOS CONFLICTOS DE JURISDICCIÓN QUE SE SUSCITAN EN LOS DELITOS INFORMÁTICOS Y LA IMPORTANCIA DE QUE ENTRE EN VIGENCIA LA LEY DE DELITOS INFORMÁTICOS".

2) El tema que investiga el Bachiller GUILLERMO AGUSTÍN LÓPEZ, es un tema de suma importancia e innovador, por el contenido técnico y científico que aporta en la materia de delitos informáticos al referirse a que el ciberespacio se reduce a Internet, la red mundial más difundida y de mayor acceso, un espacio virtual donde la gente habla por medio de servicios de conversación o chats, transmite datos mediante el correo electrónico (e-mail), compra y realiza transacciones de todo tipo, accede a información, maneja y crea información.

3) La metodología utilizada fue el método inductivo y deductivo y las técnicas de investigación fueron las entrevistas.

4) La bibliografía y leyes examinadas son las adecuadas para el profundo estudio jurídico y doctrinario del tema investigado, así mismo fue usada la investigación documental y científica, que redundan en darle un valor de obra de consulta.

5) La redacción empleada en la misma es adecuada.

Lic. ERICK ROLANDO HUITZ ENRÍQUEZ
ABOGADO Y NOTARIO
8ª. Av. 20-22 Zona 1 Oficina 8
Teléfono: 46260802

6) Los cuadros estadísticos son adecuados para el trabajo de campo realizado.

7) El contenido del trabajo de tesis, se ajusta a requerimientos científicos y técnicos que se deben cumplir de conformidad con la normativa respectiva.

8) Tanto los anexos como las conclusiones y recomendaciones dadas, son congruentes con los temas desarrollados dentro de la investigación.

9) Durante el tiempo empleado en la asesoría de la presente investigación de manera conjunta, analizamos los diferentes aspectos y procedimientos a puntualizar, en la cual ambos estuvimos de acuerdo.

10) Por la anteriormente relacionado concluyo informando a usted que procedí a ASESORAR el trabajo encomendado, por lo que me permito:

OPINAR

En definitiva el contenido del trabajo de tesis, se ajusta a requerimientos científicos y técnicos que deben cumplirse conforme la normativa respectiva, es por ello que al haberse cumplido con los requisitos establecidos en el Artículo 32 del Normativo para la Elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Público, resulta procedente emitir el presente DICTAMEN FAVORABLE, aprobando el trabajo de tesis asesorado, para que continúe su trámite hasta culminar su aprobación en el examen público de tesis.

Con las muestras de mi respeto soy de usted deferente servidor.

Lic. Erick Rolando Huitz Enríquez
Colegiado No. 7,188

Lic. Erick Rolando Huitz Enríquez
ABOGADO Y NOTARIO

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE CIENCIAS
JURÍDICAS Y SOCIALES

Ciudad Universitaria, zona 12
Guatemala, C. A.

FACULTAD DE CIENCIAS JURIDICAS Y SOCIALES
UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
SECRETARIA
Guatemala, C. A.

UNIDAD ASESORÍA DE TESIS DE LA FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES. Guatemala, veintidós de abril de dos mil diez.

Atentamente, pase al (a la) LICENCIADO (A) CARLOS MANUEL CASTRO MONROY, para que proceda a revisar el trabajo de tesis del (de la) estudiante GUILLERMO AGUSTÍN LÓPEZ, Intitulado: "LOS CONFLICTOS DE JURISDICCIÓN QUE SE SUSCITAN EN LOS DELITOS INFORMÁTICOS Y LA IMPORTANCIA DE QUE ENTRE EN VIGENCIA LA LEY DE DELITOS INFORMÁTICOS".

Me permito hacer de su conocimiento que está facultado (a) para realizar las modificaciones de forma y fondo que tengan por objeto mejorar la investigación, asimismo, del título de trabajo de tesis. En el dictamen correspondiente debe hacer constar el contenido del Artículo 32 del Normativo para la Elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Público, el cual dice: "Tanto el asesor como el revisor de tesis, harán constar en los dictámenes correspondientes, su opinión respecto del contenido científico y técnico de la tesis, la metodología y técnicas de investigación utilizadas, la redacción, los cuadros estadísticos si fueren necesarios, la contribución científica de la misma, las conclusiones, las recomendaciones y la bibliografía utilizada, si aprueban o desaprueban el trabajo de investigación y otras consideraciones que estimen pertinentes".

LIC. MARCO TULIO CASTILLO LUTÍN
JEFE DE LA UNIDAD ASESORÍA DE TESIS

cc.Unidad de Tesis
MTCL/sllh.

Lic. CARLOS MANUEL CASTRO MONROY
ABOGADO Y NOTARIO
5ta. Av. 4-29 Zona 9 – Guatemala, Ciudad
Tels. 23325867 – 56302713

FACULTAD DE CIENCIAS JURIDICAS Y SOCIALES
UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
SECRETARIA
Guatemala, C. A.

UNIDAD DE ASESORIA DE TESIS
Hora:
Firma:
11 JUN. 2010
FACULTAD DE CIENCIAS JURIDICAS Y SOCIALES

Guatemala, 11 de junio del 2010

Señor Jefe
de la Unidad de Tesis
Licenciado Marco Tulio Castillo Lutín
Facultad de Ciencias Jurídicas y Sociales de la
Universidad de San Carlos de Guatemala
Su despacho

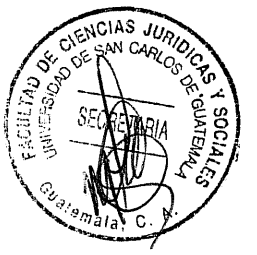
Estimado Licenciado Castillo Lutín:

Por este medio me dirijo a usted, con el propósito de informarle que de conformidad con el nombramiento que se me hiciera, para revisar la tesis del Bachiller **GUILLERMO AGUSTÍN LÓPEZ**, de fecha veintidós de abril del año en curso, respecto a su trabajo intitulado **"LOS CONFLICTOS DE JURISDICCIÓN QUE SE SUSCITAN EN LOS DELITOS INFORMÁTICOS Y LA IMPORTANCIA DE QUE ENTRE EN VIGENCIA LA LEY DE DELITOS INFORMÁTICOS"**, procedí a emitir mi opinión y los arreglos que consideré pertinentes en cuanto a su contenido, los cuales fueron atendidos por el Bachiller Agustín López.

a) El contenido científico y técnico del trabajo del ponente Agustín López es interesante, porque plantea un problema que se podría suscitar en el ámbito de los delitos informáticos, respecto a la innovación y tecnología, y la necesidad de que la protección sea más efectiva. Este es el panorama de este nuevo fenómeno científico-tecnológico en las sociedades modernas. Por ello ha llegado a sostenerse, que la Informática es hoy una forma de poder social. Las facultades que el fenómeno pone a disposición de gobiernos y de particulares, con rapidez y ahorro consiguiente de tiempo y energía, configuran un cuadro de realidades de aplicación y de posibilidades de juegos lícito e ilícito, en donde es necesario el derecho para regular los múltiples efectos de una situación, nueva y de tantas potencialidades en el medio social.

b) La metodología y técnicas utilizadas, fueron los métodos deductivo e inductivo y las técnicas tanto de entrevista como de investigación, que fueron propuestos en su plan de investigación aprobado, especialmente el método científico, que a través del análisis y la síntesis, pudo concluir la importancia de que entre en vigencia la Ley de Delitos Informáticos.

Lic. CARLOS MANUEL CASTRO MONROY
ABOGADO Y NOTARIO
5ta. Av. 4-29 Zona 9 – Guatemala, Ciudad
Tels. 23325867 – 56302713



c) La redacción utilizada considero que es adecuada al contenido científico y técnico del tema relacionado, el cual puede contribuir a que estudiosos de éste, se motiven a profundizar en la problemática planteada.

d) Se determinó que los cuadros estadísticos son adecuados por los resultados obtenidos en las entrevistas realizadas.

e) La contribución científica de este trabajo es importante, por la evolución de la tecnología dando lugar a delitos que puedan ser sancionados.

f) Las conclusiones, recomendaciones y anexos son congruentes con los hallazgos en la investigación del tema en mención.

g) La bibliografía empleada aborda en forma suficiente el tema.

h) Por lo que considero que cumple con los requisitos que para el efecto establece el Artículo 32 del Normativo para la Elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Público, y emito el presente dictamen de revisor en **forma favorable**, para que pueda continuar con el trámite correspondiente, para su posterior evaluación por el Tribunal Examinador en el Examen Público de Tesis, previo a optar al grado académico de Licenciado en Ciencias Jurídicas y Sociales.

Atentamente.

Lic. CARLOS MANUEL CASTRO MONROY
Colegiado Activo No. 3,051

Lic. Carlos Manuel Castro Monroy
ABOGADO Y NOTARIO

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE CIENCIAS
JURÍDICAS Y SOCIALES

Edificio S-7, Ciudad Universitaria
Guatemala, C. A.

FACULTAD DE CIENCIAS JURIDICAS Y SOCIALES
UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
SECRETARIA
Guatemala, C. A.

DECANATO DE LA FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES. Guatemala, treinta de marzo del año dos mil once.

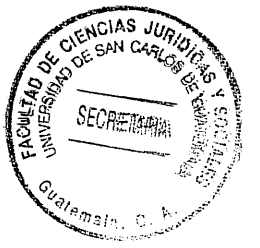
Con vista en los dictámenes que anteceden, se autoriza la Impresión del trabajo de Tesis del (de la) estudiante GUILLERMO AGUSTÍN LÓPEZ, Titulado LOS CONFLICTOS DE JURISDICCIÓN QUE SE SUSCITAN EN LOS DELITOS INFORMÁTICOS Y LA IMPORTANCIA DE QUE ENTRE EN VIGENCIA LA LEY DE DELITOS INFORMÁTICOS. Artículos 31, 33 y 34 del Normativo para la elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Público.-

0404

CMCM/sllh.

FACULTAD DE CIENCIAS JURIDICAS Y SOCIALES
UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DECANATO
Guatemala, C. A.

FACULTAD DE CIENCIAS JURIDICAS Y SOCIALES
UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
SECRETARIA
Guatemala, C. A.



DEDICATORIA

A DIOS: Por darme fortaleza para culminar mi carrera.

A MIS PADRES: CARLOS AGUSTÍN RODRÍGUEZ
CONSUELO LÓPEZ ALDANA (+)
Por todo el amor y apoyo que me brindan, sea mi triunfo para ellos.

A MIS HERMANOS Esteban,Nery,Reyna,Edgar,Ludy, Osairi, Elmer, Ester, Byron,Juan y Pahola, como un ejemplo a la dedicación y perseverancia para alcanzar el éxito.

A MIS SOBRINOS: Edwin, Mildred, Emilsa, Kimberly, Anderson y Eduardo Que este logro, los motive en sus objetivos futuros.

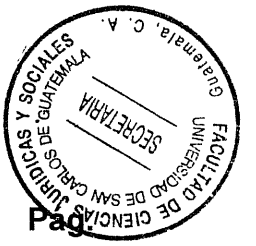
A MI FAMILIA: En general, con mucho respeto.

A MIS PADRINOS: Lic. Carlos E. Coronado G.,Lic.Jacobo Benjamin Reyes R. Por sus consejos y apoyo.

A MIS COMPAÑEROS Y AMIGOS: Con cariño. Experiencias inolvidables compartidas.

A: La tricentenaria Universidad de San Carlos de Guatemala, especialmente a la Facultad de Ciencias Jurídicas y Sociales.

A USTED: Especialmente.



ÍNDICE

Pág.

Pág.

INTRODUCCIÒN

El presente trabajo de investigación se elabora, no únicamente con el fin de dar cumplimiento a uno de los requisitos, que se exigen en la Facultad de Ciencias Jurídicas y Sociales de la Universidad de San Carlos de Guatemala, previo a optar al grado académico de Licenciado, sino también por el interés de quien escribe, acerca de la problemática que vive actualmente la sociedad guatemalteca, frente a las nuevas formas de comunicación, información y el uso de tecnologías como la Internet; los conflictos que se derivan de su utilización, como aliciente para la delincuencia en la comisión de hechos que pueden ser constitutivos de delitos.

El Código Penal data de los años 60 y 70, los cambios que ha sufrido en cuanto a reformas, no son significativos para la gama de ilícitos que se pueden cometer y los bienes jurídicos tutelados que se ven afectados, los cuales al Estado de Guatemala le corresponde proteger y que de hecho en la actualidad no lo hace, a pesar de que tal como se expone en el contenido de este trabajo, existen iniciativas de ley en el Congreso de la República, para regular de una mejor manera los delitos informáticos más comunes que se cometen en la actualidad, ya que no existe una ley específica al respecto.

Lo anterior, denota las razones por las que el autor realiza el presente trabajo, definiendo el problema como los conflictos de jurisdicción que se generan de los delitos informáticos y la falta de regulación de los mismos en forma técnica y adecuada por parte del Estado de Guatemala, incurriendo en formas de impunidad acerca de este tipo de delitos y la falta de protección en que se encuentra la sociedad guatemalteca.

Por lo anterior, la hipótesis planteada se comprobó, por cuanto, evidentemente existe conflicto jurisdiccional en el juzgamiento de este tipo de delitos, y se hace necesario por lo tanto, que se cree una ley específica que regule estos aspectos, cumpliéndose

con los objetivos de la investigación en este tipo de delitos, donde se enmarcan las conductas criminales que van dirigidas contra las computadoras, accesorios o programas como una entidad física y los supuestos de la investigación, que fueron propuestos en el plan. En el transcurso de la investigación se empleó la metodología científica, que consiste en la utilización del método deductivo-inductivo, pues se partió del estudio de todos los aspectos, que implican los hechos criminales actuales derivados del uso de tecnologías como la Internet, así también, el método de análisis y síntesis, desplazando todo el conocimiento en partes para su estudio y posteriormente, uniéndolo de manera de llegar a conclusiones respecto al tema investigado. Con respecto a las técnicas, fueron fundamentales las bibliográficas en cuanto a la consulta de libros y las estadísticas que se utilizaron en la presentación del trabajo de campo.

El trabajo para una mayor comprensión se ha dividido en cuatro capítulos: En el primero, se hace una relación breve acerca de la Internet y las nuevas tecnologías; en el segundo capítulo, lo relativo a los delitos informáticos, tanto los que se regulan en el Código Penal, como los que se regulan en la legislación comparada; en el capítulo tercero, se establecen aspectos generales de la iniciativa de ley, que contiene la Ley de delitos informáticos y los conflictos de jurisdicción, que se plantean actualmente y lo que sucede también en la legislación comparada, para que en el capítulo cuarto, se establezcan los resultados del trabajo de campo, las ventajas de que entre en vigencia la ley en iniciativa que se hace referencia, y los aspectos que la misma debe considerar y mejorar, de acuerdo a la realidad y a los resultados de la investigación bibliográfica, documental y de campo.

Por la tanto se considera que el presente trabajo, puede ser motivo suficiente para futuros estudios que se realicen de manera más profunda y sistematizada sobre los delitos informáticos y los problemas que se derivan del uso de la Internet.

CAPÍTULO I

1. El derecho informático

1.1 Breves antecedentes

Es innegable reconocer que estamos desde hace tiempo, inmersos dentro de un mundo digital, tecnológico. Las personas cuando escuchan la palabra Internet, automáticamente la asocian con las computadoras, y está claro, porque para entrar a ese mundo digital, se necesita de esta herramienta.

El Internet entonces, constituye una forma de comunicación que fue inventada recientemente y que ha producido gran impacto en la vida social en los distintos ámbitos, y en el caso de Guatemala, que hasta hace poco tiempo, aproximadamente en los años 70, se empezó a utilizar esta forma de uso principalmente para facilitar la tarea laboral, en el caso de las impresiones, estudios, casos, guardar información, etc., y que con el aparecimiento de esta forma de redes de comunicación, se ha incrementado enormemente su uso, siendo que en la actualidad, cualquier persona que adquiera una computadora, puede tener acceso al Internet.

Representa su uso entonces ventajas para la sociedad, aunque también desventajas, principalmente en el ámbito de la criminalidad. El ajuste de medidas estatales para su regulación, como el ente rector de la paz y quien es el llamado para sancionar conductas ilícitas, que se puedan cometer en lesión a bienes jurídicos tutelados y como se verá más adelante, existen muchos delitos los cuales el Estado de Guatemala, no se ha motivado en regular, por lo que se considera que no ha estado a la vanguardia de estos avances, y que han generado la violación a los derechos fundamentales de las personas, pero que no son sancionadas estas conductas, ni mucho menos perseguidas, por cuanto no se encuentran reguladas en el Código Penal como figuras delictivas.

Existe una gran gama de figuras ilícitas que se cometen a diario con el uso del Internet y que esas conductas, aunque sean dañinas para las personas a quienes se les afecta, no se pueden sancionar, por una serie de circunstancias que también se analizarán más adelante, pero fundamentalmente, una de ellas, es la falta de regulación en la ley. En este caso, también se encuentran los denominados metatags que son las palabras del lenguaje HTML, que pueden ser leídas solamente por los motores de búsqueda de la red, y que describen el contenido del sitio en el que se encuentran, de forma que pueden ser localizados y obtenidos por los usuarios interesados.

Si su empleo se realiza con el propósito de conducir a los usuarios a las páginas de los competidores, entonces constituye un acto de carácter ilícito, provocando así un riesgo de asociación o confusión, en cuyo caso resultan de aplicación, las normas de competencia desleal y que por esa situación a juicio de quien escribe, tal como se describen, deben ser regulados como delito en el Código Penal Guatemalteco.

1.2 Definición de derecho informático

La información acerca del Internet como tal, no se encuentra aún en libros del derecho. El Internet es: "un conjunto descentralizado de redes de comunicación interconectadas, que utilizan la familia de protocolos TCP/IP, garantizando que las redes físicas heterogéneas que la componen funcionen como una red lógica única, de alcance mundial".[1]

Derecho informático entonces, es aquel conjunto de normas jurídicas, principios, instituciones que tienen relación directa con el uso de las tecnologías a través del Internet y que facilitan las comunicaciones, previendo un marco regulatorio con el fin de evitar los abusos a que puedan estar expuestos los usuarios del mismo, como un deber del Estado.

[1] Sandoval Ramírez, Luis. **La computación en el siglo veinte**. Pág. 24

1.3 Antecedentes históricos del aparecimiento del Internet a nivel mundial

Sus orígenes se remontan a 1969, cuando se estableció la primera conexión de computadoras, conocida como ARPANET, entre tres universidades en California y una en Utah, Estados Unidos.

Uno de los servicios que más éxito ha tenido en Internet, ha sido la World Wide Web (www, o "la Web"), hasta tal punto que es habitual la confusión entre ambos términos. La www es un conjunto de protocolos que permite, de forma sencilla, la consulta remota de archivos de hipertexto. Ésta fue un desarrollo posterior (1990) y utiliza Internet como medio de transmisión.

Existen muchos otros servicios y protocolos en Internet, aparte de la Web: El envío de correo electrónico (SMTP), la transmisión de archivos (FTP y P2P), las conversaciones en línea (IRC), la mensajería instantánea y presencia, la transmisión de contenido y comunicación multimedia-telefonía (VoIP), televisión (IPTV), los boletines electrónicos (NNTP), el acceso remoto a otras máquinas (SSH y Telnet) o los juegos en línea.

En el mes de julio de 1961, Leonard Kleinrock publicó desde el MIT el primer documento sobre la teoría de conmutación de paquetes. Kleinrock convenció a Lawrence Roberts, de la factibilidad teórica de las comunicaciones vía paquetes en lugar de circuitos, lo cual resultó ser un gran avance en el camino hacia el trabajo informático en red.

El otro paso fundamental, fue hacer dialogar a los ordenadores entre sí. Para explorar este terreno, en 1965, Roberts conectó una computadora TX2 en Massachusetts, con un Q-32 en California a través de una línea telefónica conmutada de baja velocidad, creando así, la primera (aunque reducida) red de computadoras de área amplia jamás construida.

En 1969, la primera red interconectada nace el 21 de noviembre de 1969, cuando se crea el primer enlace entre las universidades de UCLA y Stanford por medio de la línea telefónica conmutada, gracias a los trabajos y estudios anteriores de varios científicos y organizaciones desde 1959. El mito de que ARPANET, la primera red, se construyó simplemente para sobrevivir a ataques nucleares sigue siendo muy popular. Sin embargo, éste no fue el único motivo. Si bien es cierto que ARPANET fue diseñada para sobrevivir a fallos en la red, la verdadera razón para ello, era que los nodos de conmutación eran poco fiables, tal y como se atestigua en la siguiente cita:

A raíz de un estudio de RAND, se extendió el falso rumor de que ARPANET fue diseñada para resistir un ataque nuclear. Esto nunca fue cierto, solamente un estudio de RAND, no relacionado con ARPANET, consideraba la guerra nuclear en la transmisión segura de comunicaciones de voz. Sin embargo, trabajos posteriores enfatizaron la robustez y capacidad de supervivencia, de grandes porciones de las redes subyacentes.

En 1972, se realizó la primera demostración pública de ARPANET, una nueva red de comunicaciones financiada por la DARPA, que funcionaba de forma distribuida sobre la red telefónica conmutada. El éxito de esta nueva arquitectura, sirvió para que en 1973, la DARPA iniciara un programa de investigación sobre posibles técnicas para interconectar redes (orientadas al tráfico de paquetes) de distintas clases. Para este fin, desarrollaron nuevos protocolos de comunicaciones, que permitiesen este intercambio de información de forma "transparente" para las computadoras conectadas. De la filosofía del proyecto, surgió el nombre de "Internet", que se aplicó al sistema de redes interconectadas mediante los protocolos TCP e IP.

En 1983, el 1 de enero, ARPANET cambió el protocolo NCP por TCP/IP. Ese mismo año, se creó el IAB con el fin de estandarizar el protocolo TCP/IP y de proporcionar recursos de investigación a Internet. Por otra parte, se centró la función de

asignación de identificadores en la IANA, que más tarde delegó parte de sus funciones, en el Internet registry que, a su vez, proporciona servicios a los DNS.

En 1986, la NSF comenzó el desarrollo de NSFNET, que se convirtió en la principal red en árbol de Internet, complementada después con las redes NSINET y ESNET, todas ellas en Estados Unidos. Paralelamente, otras redes troncales en Europa, tanto públicas como comerciales, junto con las americanas formaban el esqueleto básico ("backbone") de Internet.

En 1989, con la integración de los protocolos OSI en la arquitectura de Internet, se inició la tendencia actual de permitir, no sólo la interconexión de redes de estructuras dispares, sino también la de facilitar el uso de distintos protocolos de comunicaciones.

En el CERN de Ginebra, un grupo de físicos encabezado por Tim Berners Lee, creó el lenguaje HTLM basado en el SGML. En 1990 el mismo equipo, construyó el primer cliente Web, llamado WorldWideWeb (www), y el primer servidor Web.

En 2006, el 3 de enero, Internet alcanzó los mil cien millones de usuarios. Se prevé que en diez años, la cantidad de navegantes de la red aumentará a dos mil millones.

El Internet tiene un impacto profundo en el trabajo, el ocio y el conocimiento a nivel mundial. Gracias a la Web, millones de personas tienen acceso fácil e inmediato a una cantidad extensa y diversa de información en línea. Un ejemplo de esto, es el desarrollo y la distribución de colaboración del software de Free/Libre/Open-Source (SEDA) por ejemplo GNU, Linux, Mozilla y OpenOffice.org.

Al hacer una comparación a las enciclopedias y a las bibliotecas tradicionales, la Web ha permitido una descentralización repentina y extrema, de la información y de los datos. Algunas compañías e individuos, han adoptado el uso de los Weblog, que se utilizan en gran parte como diarios actualizables. Algunas organizaciones

comerciales, animan a su personal para incorporar sus áreas de especialización en sus sitios, con la esperanza de que impresionen a los visitantes con conocimiento experto e información libre.

El Internet, ha llegado a gran parte de los hogares y de las empresas de los países ricos, en este aspecto se ha abierto una brecha digital con los países pobres, en los cuales la penetración de Internet y las nuevas tecnologías es muy limitada para las personas.

No obstante, en el transcurso del tiempo se ha venido extendiendo, el acceso a Internet en casi todas las regiones del mundo, de modo que es relativamente sencillo, encontrar por lo menos dos computadoras conectadas en regiones remotas.

Desde una perspectiva cultural del conocimiento, Internet ha sido una ventaja y una responsabilidad. Para la gente que está interesada en otras culturas, la red de redes, proporciona una cantidad significativa de información y de una interactividad que sería inasequible de otra manera.

El Internet entró como una herramienta de globalización, poniendo fin al aislamiento de culturas. Debido a su rápida masificación e incorporación en la vida del ser humano, el espacio virtual es actualizado constantemente, de información fidedigna o irrelevante.

Muchos utilizan el Internet para descargar música, películas y otros trabajos. Hay fuentes que cobran por su uso y otras son gratuitas, usando los servidores centralizados y distribuidos, las tecnologías de P2P. Otros utilizan la red para tener acceso a las noticias y el estado del tiempo.

La mensajería instantánea o chat y el correo electrónico, son algunos de los servicios de uso más extendido. En muchas ocasiones, los proveedores de dichos servicios brindan a sus afiliados servicios adicionales, como la creación de espacios y perfiles

públicos, en donde los internautas tienen la posibilidad de colocar en la red, fotografías y comentarios personales. Se especula actualmente, si tales sistemas de comunicación fomentan o restringen, el contacto de persona a persona entre los seres humanos.

En tiempos más recientes han cobrado auge sitios como YouTube, en donde los usuarios pueden tener acceso a una gran variedad de videos, sobre prácticamente cualquier tema.

"La pornografía representa buena parte del tráfico en Internet, siendo a menudo un aspecto controversial de la red, por las implicaciones morales que le acompañan. Proporciona a menudo, una fuente significativa del rédito de publicidad para otros sitios. Muchos gobiernos, hàn procurado sin éxito poner restricciones en el uso de ambas industrias en Internet. Un área principal del ocio en la Internet es el sistema multijugador".[2]

A través de la información se puede saber, qué es lo que significa y la historia o evolución que ha tenido esta forma de comunicación a nivel mundial, que ha representado no solo beneficios, sino también perjuicios. Cabría señalar entonces, que el Estado en este caso, determinará los perjuicios para contrarrestarlos en beneficio precisamente de la población guatemalteca.

A pesar que desde sus inicios el Internet, sirvió para navegar respecto a algo muy concreto, como buscar información didáctica, información para ampliar conocimientos acerca de determinado tema; en la actualidad, la oportunidad de escritores de publicar a través de este sistema sus ideas, obras, etc., venderlas, comercializar productos, objetos, bienes, etc., también ha significado el interés de los criminales, para provocar perjuicios con fines lucrativos a la sociedad que utiliza este servicio.

[2] www.wikipedia.com.htlm. **Enciclopedia wikipedia.** Día de consulta: 2-3-2010

Su existencia es relativamente reciente, como se ha observado en el análisis histórico, la incorporación de tantas personas a la red, hace que este fenómeno vaya en incremento a través del tiempo, tan es así, que se ha reducido el uso del teléfono, del manuscrito para hacer cartas a los parientes, amigos, etc., ya que resulta mucho más cómodo que desde sus hogares o de sus trabajos, puedan comunicarse de un país muy lejano al otro y viceversa.

Como toda gran revolución, Internet augura una nueva era de diferentes métodos de resolución de problemas. Algunos sienten que Internet, produce la sensación que todos han sentido alguna vez, produce la esperanza que se necesita cuando se quiere conseguir algo. Es un despertar de intenciones, que jamás antes la tecnología había logrado en la población mundial. Para algunos usuarios, Internet genera una sensación de cercanía, empatía, comprensión, y a la vez de confusión, discusión, lucha y conflictos que ellos mismos denominan como la vida misma.

Con la aparición de Internet y de las conexiones de alta velocidad disponibles al público, Internet ha alterado de manera significativa, la manera de trabajar de algunas personas, al poder hacerlo desde sus respectivos hogares. Internet ha permitido a estas personas, mayor flexibilidad en términos de horarios y de localización, contrariamente a la jornada laboral tradicional de nueve a cinco, en la cual los empleados se desplazan al lugar de trabajo.

Un experto contable asentado en un país, puede revisar los libros de una compañía en otro país, en un servidor situado en un tercer país, que sea mantenido remotamente por los especialistas en un cuarto. Internet y sobre todo los blogs, han dado a los trabajadores un foro, en el cual pueden expresar sus opiniones sobre sus empleos, jefes y compañeros, creando una cantidad masiva de información y de datos sobre el trabajo, que está siendo recogido actualmente por el colegio de abogados de Harvard.

"El Internet ha impulsado el fenómeno de la globalización y junto con la llamada desmaterialización de la economía, ha dado lugar al nacimiento de una nueva economía, caracterizada por la utilización de la red en todos los procesos de incremento de valor de la empresa".[3] Respecto al acceso a Internet, incluye aproximadamente 5,000 redes en todo el mundo y más de 100 protocolos distintos basados en TCP/IP, que se configura como el protocolo de la red. Los servicios disponibles en la red mundial de PC, han avanzado mucho gracias a las nuevas tecnologías de transmisión de alta velocidad, como DSL y Wireless, y se ha logrado unir a las personas con videoconferencia, ver imágenes por satélite (ver su casa desde el cielo), observar el mundo por Webcams, hacer llamadas telefónicas gratuitas, o disfrutar de un juego multijugador en 3D, un buen libro PDF, o álbumes y películas para descargar.

El método de acceso a Internet vigente hace algunos años, la telefonía básica, ha venido siendo sustituida gradualmente por conexiones más veloces y estables, entre ellas el ADSL, Cable Módems, o el RDSI. También han aparecido formas de acceso a través de la red eléctrica, e incluso por satélite (generalmente, sólo para descarga, aunque existe la posibilidad de doble vía, utilizando el protocolo DVB-RS).

"El Internet, también está disponible en muchos lugares públicos tales como bibliotecas, hoteles, o cibercafés y hasta en shoppings. Una nueva forma de acceder sin necesidad de un puesto fijo, son las redes inalámbricas, hoy presente en aeropuertos, subterráneos, universidades o poblaciones enteras".[4]

1.4 Definición de delitos informáticos

El autor mexicano Julio Téllez Valdez, señala que los delitos informáticos son: "actitudes ilícitas en que se tienen a las computadoras como instrumento o fin

[3] www.monografias.com.htlm. Día de consulta: 2-3-2010
[4] www.wikipedia.com.htlm. **Historia del Internet y su evolución**. Día de consulta: 3-3-2010

(concepto atípico) o las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin (concepto típico)". [5]

Por su parte, el tratadista penal italiano Carlos Sarzana, sostiene que los delitos informáticos son: "cualquier comportamiento criminal en que la computadora está involucrada como material, objeto o mero símbolo". [6]

Se puede definir a los delitos informáticos como: "aquellas acciones típicas, antijurídicas y culpables, que recaen sobre la información, atentando contra su integridad, confidencialidad o disponibilidad, como bien jurídico de naturaleza colectiva o macro-social (abarcativo de otros intereses, vgr.: propiedad común, intimidad, propiedad intelectual, seguridad pública, confianza en el correcto funcionamiento de los sistemas informáticos, etc.), en cualquiera de las fases que tienen vinculación con su flujo o intercambio (ingreso, almacenamiento, proceso, transmisión y/o egreso), contenida en sistemas informáticos de cualquier índole, sobre los que operan las maniobras dolosas".[7]

Entonces, puede concluirse en cuanto a la definición de los delitos informáticos, que estos son aquellos ilícitos que se cometen utilizando como herramienta la computadora y los mecanismos de comunicación, entre ellos, el Internet, y que ocasionan perjuicio a terceros, respecto a la lesión que se produce a bienes jurídicos tutelados por el Estado previamente y los que aún no se encuentran amparados legalmente.

Por otro lado, el Consejo de Europa ha definido a los delitos informáticos como: "toda representación de hechos, información o conceptos en un formato que pueda ser procesado a través de un sistema informático, incluyendo un programa que puede hacer que un sistema informático realice una función".[8]

---

[5] Téllez Valdez, Julio. **Los delitos informáticos**. Pág. 246
[6] Ibíd. Pág. 246
[7] Carrión, Hugo Daniel. **Presupuestos para la incriminación del Hawking**. Pág. 2
[8] www.ceue.com.htlm. Consejo de Europa. **Comité Europeo para los problemas de la delincuencia 25 de mayo 2001**. Día de consulta: 1-3-2010.

De conformidad con lo anterior, se debe entender entonces que los delitos informáticos en general, son aquellos actos delictivos realizados con el uso de computadoras o medios electrónicos, cuando tales conductas constituyen el único medio de comisión posible -o el considerablemente más efectivo-, y los delitos en que se daña estos equipos, redes informáticas, o la información contenida en ellos, vulnerando bienes jurídicos protegidos y cuyas conductas ilícitas, se encuentren previamente establecidas en el país en donde se produjo la afectación o el daño.

En términos generales, entonces, se debe comprender que estos delitos se cometen utilizando los medios tecnológicos o son el método o medio comisivo, o el fin de la conducta delictiva.

Por lo anterior, es comprensible que los delitos informáticos se manifiesten en dos sentidos: como delitos de resultado y como delitos de medio. En el primer caso, porque las conductas que vulneran los sistemas que utilizan tecnologías de información, lesionan el bien jurídico constituido por la información que los sistemas contienen, procesan, resguardan y transmiten, puesto que la información no es más que el bien que subyace en ellos.

En el segundo caso, porque recoge las conductas que se valen del uso de las tecnologías de información, para atentar contra bienes jurídicos distintos de la información contenida y tratada en sistemas automatizados, esto es, bienes como la propiedad, la privacidad de las personas o el orden económico. Lo que distingue a este grupo de delitos informáticos, es la utilización de las tecnologías de información, como único medio de comisión posible o como medio extremadamente ventajoso, en relación con cualquier otro para vulnerar el bien jurídico objeto de protección penal.

Según el autor Téllez Valdez al cual se referirá en este trabajo, que ha sido uno de los máximos exponentes en esta materia, este tipo de acciones presentan las siguientes características principales:

a) "Son conductas criminales de cuello blanco (white collar crime), en tanto que sólo un determinado número de personas con ciertos conocimientos (en este caso técnicos), pueden llegar a cometerlas.

b) Son acciones ocupacionales, en cuanto a que muchas veces se realizan cuando el sujeto se halla trabajando.

c) Son acciones de oportunidad, ya que se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico.

d) Provocan serias pérdidas económicas, ya que casi siempre producen beneficios de más de cinco cifras a aquellos que las realizan.

e) Ofrecen posibilidades de tiempo y espacio, ya que en milésimas de segundo y sin una necesaria presencia física, pueden llegar a consumarse.

f) Son muchos los casos y pocas las denuncias, y todo ello debido a la misma falta de regulación por parte del derecho.

g) Son muy sofisticados y relativamente frecuentes en el ámbito militar.

h) Presentan grandes dificultades para su comprobación, esto por su mismo carácter técnico.

i) En su mayoría son imprudenciales y no necesariamente se cometen con intención.

j) Ofrecen facilidades para su comisión a los menores de edad.

k) Tienden a proliferar cada vez más, por lo que requieren una urgente regulación.

l) Por el momento siguen siendo ilícitos, impunes de manera manifiesta ante la ley".

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

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

a) Falsificación de documentos vía computarizada (tarjetas de crédito, cheques, etc.).

b) Variación de los activos y pasivos en la situación contable de las empresas.

c) Planeamiento y simulación de delitos convencionales (robo, homicidio, fraude, etc.).

d) Lectura, sustracción o copiado de información confidencial.

e) Modificación de datos tanto en la entrada como en la salida.

f) Aprovechamiento indebido o violación de un código, para penetrar a un sistema introduciendo instrucciones inapropiadas.

g) Variación en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta bancaria apócrifa.

h) Uso no autorizado de programas de cómputo.

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

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

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

l) Acceso a áreas informatizadas en forma no autorizada.

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

2) Como un fin u objetivo: En este tipo de delitos o categoría, se enmarcan las conductas criminales que van dirigidas contra las computadoras, accesorios o programas como entidad física, como por ejemplo:

a) Programación de instrucciones que producen un bloqueo total al sistema.

b) Destrucción de programas por cualquier método.

c) Daño a la memoria.

d) Atentado físico contra la máquina o sus accesorios.

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

f) Secuestro de soportes magnéticos entre los que figure información valiosa con fines de chantaje (pago de rescate, etc.).

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

a) Acceso no autorizado: Uso ilegítimo de passwords y la entrada de un sistema informático sin la autorización del propietario.

b) Destrucción de datos: Los daños causados en la red mediante la introducción de virus, bomba lógica, etc.

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

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

e) Estafas electrónicas: A través de compras realizadas haciendo uso de la red. Transferencias de fondos: Engaños en la realización de este tipo de transacciones.

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

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

b) Terrorismo: Mensajes anónimos aprovechados por grupos terroristas para remitir consignas y planes de actuación a nivel internacional.

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

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

De conformidad con lo mencionado por el autor Téllez Valdez, se debe entender entonces que los delitos informáticos analizados en un aspecto general, son aquellos

actos delictivos realizados con el uso de medios electrónicos, vulnerando bienes jurídicos protegidos y cuyas conductas ilícitas, se encuentren previamente establecidas en el país en donde se produjo la afectación o el daño.

Entonces se debe comprender que estos delitos, se cometen utilizando los medios tecnológicos o son el método o medio comisivo, o el fin de la conducta delictiva.

CAPÍTULO II

2. Los delitos informáticos que se regulan en la legislación penal guatemalteca y los que hacen falta por regular

2.1 Sujetos activos y pasivos de los delitos informáticos

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

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

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

El nivel típico de aptitudes del delincuente informático es tema de controversia, ya que para algunos, el nivel de aptitudes no es indicador de delincuencia informática, en tanto que otros, aducen que los posibles delincuentes informáticos son personas

listas, decididas, motivadas y dispuestas a aceptar un reto tecnológico; características que pudieran encontrarse en un empleado del sector de procesamiento de datos.

"Sin embargo, teniendo en cuenta las características ya mencionadas de las personas que cometen los "delitos informáticos", los estudiosos en la materia los han catalogado como "delitos de cuello blanco" término introducido por primera vez por el criminólogo norteamericano Edwin Sutherland en el año de 1943".[9]

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

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

Es difícil elaborar estadísticas sobre ambos tipos de delitos. Sin embargo, la cifra es muy alta; no es fácil descubrirlo y sancionarlo en razón del poder económico de quienes los cometen, pero los daños económicos son altísimos; existe una gran indiferencia de la opinión pública sobre los daños ocasionados a la sociedad: la sociedad no considera delincuentes a los sujetos que cometen este tipo de delitos,

[9] Téllez Valdez, Julio. **Los delitos informáticos**. Pág. 235

no los segrega, no los desprecia, ni los desvaloriza; por el contrario, el autor o autores de este tipo de delitos, se consideran así mismos respetables, otra coincidencia que tienen estos tipos de delitos es que generalmente, son objeto de medidas o sanciones de carácter administrativo y no privativos de la libertad.

Este nivel de criminalidad, se puede explicar por la dificultad de reprimirla en forma internacional, ya que los usuarios están esparcidos por todo el mundo, y en consecuencia, existe una posibilidad muy grande de que el agresor y la víctima, estén sujetos a leyes nacionales diferentes. Además, si bien los acuerdos de cooperación internacional y los tratados de extradición bilaterales, intentan remediar algunas de las dificultades ocasionadas por los delitos informáticos, sus posibilidades son limitadas.

En lo que se refiere a delitos informáticos, Oliver Hance considera tres categorías de comportamiento, que pueden afectar negativamente a los usuarios de los sistemas informáticos. Las mismas son las siguientes:

"1) Acceso no autorizado: Es el primer paso de cualquier delito. Se refiere a un usuario que, sin autorización, se conecta deliberadamente a una red, un servidor o un archivo (por ejemplo, una casilla de correo electrónico), o hace la conexión por accidente, pero decide voluntariamente mantenerse conectado.

2) Actos dañinos o circulación de material dañino: Una vez que se conecta a un servidor, el infractor puede robar archivos, copiarlos o hacer circular información negativa, como virus o gusanos. Tal comportamiento, casi siempre es clasificado como piratería (apropiación, descarga y uso de la información sin conocimiento del propietario), o como sabotaje (alteración, modificación o destrucción de datos o de software, uno de cuyos efectos es paralizar la actividad del sistema o del servidor en Internet).

3) Interceptación no autorizada: En este caso, el hacker detecta pulsos electrónicos transmitidos por una red o una computadora y obtiene información no dirigida a él. Las leyes estadounidenses y canadienses, lo mismo que los sistemas legales de la mayoría de los países europeos, han tipificado y penalizado estos tres tipos de comportamiento ilícito, cometidos a través de las computadoras". [10]

Por su parte, el Manual de Naciones Unidas para la Prevención y Control de Delitos Informáticos "señala, que cuando el problema se eleva a la escena internacional, se magnifican los inconvenientes y las insuficiencias, por cuanto los delitos informáticos constituyen, una nueva forma de crimen transnacional y su combate requiere de una eficaz cooperación internacional concertada".[11]

Asimismo la ONU resume de la siguiente manera, los problemas que rodean a la cooperación internacional en el área de los delitos informáticos:

a) Falta de acuerdos globales acerca de que tipo de conductas deben constituir delitos informáticos.

b) Ausencia de acuerdos globales en la definición legal de dichas conductas delictivas.

c) Falta de especialización de las policías, fiscales y otros funcionarios judiciales, en el campo de los delitos informáticos.

d) No armonización entre las diferentes leyes procesales nacionales, acerca de la investigación de los delitos informáticos.

e) Carácter transnacional de muchos delitos, cometidos mediante el uso de computadoras.

---

[10] Hance, Oliver. **Leyes y negocios en Internet**. Pág. 98
[11] www.onu.com.htlm. **Manual de Naciones Unidas para la Prevención y Control de Delitos Informáticos**. Día de consulta: 3-3-2010

f) Ausencia de tratados de extradición, acuerdos de ayuda mutuos y de mecanismos sincronizados, que permitan la puesta en vigor de la cooperación internacional.

En síntesis es destacable que la delincuencia informática, se apoya en el delito instrumentado por el uso de la computadora, a través de redes telemáticas y la interconexión de la computadora, aunque no es el único medio.

Las ventajas y las necesidades de que exista un flujo nacional e internacional de datos, y que aumenta de modo creciente en los países, conlleva también a la posibilidad creciente de estos delitos; por eso puede señalarse que la criminalidad informática, constituye un reto considerable tanto para los sectores afectados de la infraestructura crítica de un país, como para los legisladores, las autoridades policiales encargadas de las investigaciones y los funcionarios judiciales.

Muchas de las personas que cometen los delitos informáticos, poseen ciertas características específicas, tales como la habilidad para el manejo de los sistemas informáticos o la realización de tareas laborales, que le facilitan el acceso a información de carácter sensible.

En algunos casos la motivación del delito informático no es económica, sino que se relaciona con el deseo de ejercitar, y a veces dar a conocer a otras personas, los conocimientos o habilidades del delincuente en ese campo.

Ahora bien, el sujeto pasivo en el caso de los delitos informáticos, pueden ser individuos, instituciones crediticias, órganos estatales, etc. que utilicen sistemas automatizados de información, generalmente conectados a otros equipos o sistemas externos.

2.2 Los delitos informáticos en la legislación penal guatemalteca

En materia propiamente de los delitos informáticos, en el Capítulo VII del Código Penal Decreto Número 17-73 se adicionaron algunas figuras delictivas en forma muy generalizada, como se observará e incluidas dentro de los delitos contra los derechos de autor y propiedad intelectual, sin que puedan tener una relación directa entre éstos y los otros, tal como se observa con el análisis anterior, sin embargo, se han establecido y a continuación se describen las mismas:

Artículo 274 "A". Destrucción de registros informáticos. "Será sancionado con prisión de seis meses a cuatro años, y multa de doscientos a dos mil quetzales, el que destruyere, borrare o de cualquier modo inutilizare registros informáticos".

Artículo 274 "B". Alteración de programas. "La misma pena del artículo anterior se aplicará al que alterare, borrare o de cualquier modo inutilizare las instrucciones o programas que utilizan las computadoras".

Artículo 274 "C". Reproducción de instrucciones o programas de computación. "Se impondrá prisión de seis meses a cuatro años y multa de quinientos a dos mil quinientos quetzales al que, sin autorización del autor, copiare o de cualquier modo reprodujere las instrucciones o programas de computación".

Artículo 274 "D". Registros prohibidos. "Se impondrá prisión de seis meses a cuatro años y multa de doscientos a mil quetzales, al que creare un banco de datos o un registro informático con datos que puedan afectar la intimidad de las personas".

Artículo 274 "E". Manipulación de información. "Se impondrá prisión de uno a cinco años y multa de quinientos a tres mil quetzales, al que utilizare registros informáticos o programas de computación para ocultar, alterar o distorsionar información requerida para una actividad comercial, para el cumplimiento de una obligación

respecto al Estado o para ocultar, falsear o alterar los estados contables o la situación patrimonial de una persona física o jurídica".

Artículo 274 "F". Uso de información. "Se impondrá prisión de seis meses a dos años, y multa de doscientos a mil quetzales al que, sin autorización, utilizare los registros informáticos de otro, o ingresare, por cualquier medio, a su banco de datos o archivos electrónicos".

Artículo 274 "G". Programas destructivos. "Será sancionado con prisión de seis meses a cuatro años, y multa de doscientos a mil quetzales, al que distribuyere o pusiere en circulación programas o instrucciones destructivas, que puedan causar perjuicio a los registros, programas o equipos de computación".

Como se observa con las anteriores figuras delictivas, es evidente que falta mucho por regular, y específicamente por el hecho, de que la tecnología se encuentra en constante cambio y evolución, y las nuevas conductas que surgen en materia de informática, deben regularse, para evitar la transgresión a derechos fundamentales de las personas.

2.3 Figuras delictivas, que si bien están reguladas en el Código Penal, son susceptibles de cometerse utilizando medios informáticos

Dentro de las figuras delictivas que no solamente se cometen tal como lo regulan las normas, sino que pueden hacerse a través del uso del Internet y que no se regulan, entre ellas las más importantes son las siguientes:

2.3.1 La coacción y amenazas

Artículo 214. Coacción. "Quien sin estar legítimamente autorizado, mediante procedimiento violento, intimidatorio o que en cualquier forma compela a otro, obligue a éste para que haga o deje de hacer lo que la ley no le prohíbe, efectúe o consienta

lo que no quiere o que tolere que otra persona lo haga, sea justo o no, será sancionado con prisión de seis meses a dos años".

Artículo 215. Amenazas. "Quien amenazare a otro con causar a él mismo o a sus parientes, dentro de los grados de ley, en su persona, honra o propiedad, un mal que constituya o no delito, será sancionado con prisión de seis meses a tres años".

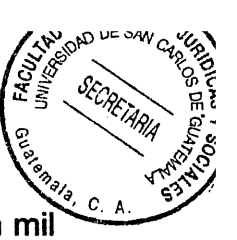
Artículo 216. Coacción contra la libertad política. "Quien fuera de los casos previstos en las leyes especiales respectivas, por medio de violencias o amenazas impidiere o coartare el ejercicio de cualquier derecho político, será sancionado con prisión de seis meses a tres años".

Con relación a las anteriores figuras delictivas que se refieren a la coacción y a las amenazas, es evidente de que éstas pueden producirse no de manera tradicional, de boca a boca entre un sujeto activo y un sujeto pasivo, sino que puede hacerse a través del uso de las herramientas de la computadora, en los mensajes de texto, en los teléfonos celulares, y cualquier otro medio digital, por lo que estas figuras debieran sufrir los cambios que ameritan.

2.3.2 De la violación y revelación de secretos

Artículo 217. Violación de correspondencia y papeles privados. "Quien a propósito o para descubrir los secretos de otro, abriere correspondencia, pliego cerrado o despachos telegráficos, telefónico o de otra naturaleza, que no le estén dirigidos o a quien, sin abrirlos, se impusiere de su contenido, será sancionado con multa de cien a un mil quetzales".

Artículo 218. Sustracción, desvío o supresión de correspondencia. "Quien, indebidamente, se apoderare de correspondencia, pliego o despachos, a que se refiere el artículo anterior o de otro papel privado, aunque no estén cerrados o quien



los suprimiere o desviare de su destino, será sancionado con multa de cien a un mil quetzales".

Artículo 219. Intercepción o reproducción de comunicaciones. "Quien, valiéndose de medios fraudulentos interceptare, copiare o grabare comunicaciones televisadas, radiales, telegráficas, telefónicas u otras semejantes o de igual naturaleza, o las impida o interrumpa, será sancionado con multa de cien a un mil quetzales".

Artículo 220. Agravación específica. "Las sanciones señaladas para los hechos delictuosos definidos en los tres artículos que preceden, serán de prisión de seis meses a tres años, en los siguientes casos:

1o. Si el autor se aprovechare de su calidad de funcionario o empleado de la dependencia, empresa o entidad respectivas.

2o. Si se tratare de asuntos oficiales.

3o. Si la información obtenida, el autor la hiciere pública, por cualquier medio".

Artículo 222. Publicidad indebida. "Quien, hallándose legítimamente en posesión de correspondencia, de papeles o de grabaciones, fotografías no destinadas a la publicidad, los hiciere públicos, sin la debida autorización, aunque le hubieren sido dirigidos, cuando el hecho cause o pudiere causar perjuicio, será sancionado con multa de doscientos a dos mil quetzales".

Artículo 223. Revelación de secreto profesional. "Quien, sin justa causa, revelare o empleare en provecho propio o ajeno un secreto del que se ha enterado por razón de su estado, oficio, empleo, profesión o arte, sin que con ello ocasionare o pudiere ocasionar perjuicio, será sancionado con prisión de seis meses a dos años o multa de cien a un mil quetzales".

Artículo 241. Usurpación de estado civil. "Quien, usurpare el estado civil de otro, será sancionado con prisión de dos a cinco años".

En los delitos anteriormente señalados, también puede observarse la complejidad de los supuestos y que no se refieren, a como pueden producirse con el uso de las tecnologías a través del Internet y que ello, necesariamente ocasiona un perjuicio a los particulares, que son víctimas de estos abusos e ilegalidades.

2.3.3 De los delitos contra el patrimonio

Artículo 246. Hurto. "Quien tomare, sin la debida autorización cosa, mueble, total o parcialmente ajena, será sancionado con prisión de 1 a 6 años".

Artículo 247. Hurto agravado. "Es hurto agravado:

1o. El cometido por doméstico o interviniendo grave abuso de confianza.

2o. Cuando fuere cometido aprovechándose de calamidad pública o privada, o de peligro común.

3o. Cuando se cometiere en el interior de casa, habitación o morada o para ejecutarlo el agente se quedare subrepticiamente en edificio o lugar destinado a habitación. Esta circunstancia agravante no se aplicará cuando el hurto concursare con el de allanamiento de morada.

4o. Cuando se cometiere usando ganzúa, llave falsa u otro instrumento semejante o llave verdadera que hubiere sido sustraída, hallado o retenida.

5o. Cuando participaren en su comisión dos o más personas; una o varias fingiéndose autoridad o jefes o empleados de un servicio público.

6o. Cuando el hurto fuere de objetos o dinero de viajeros y se realizare en cualquier clase de vehículos o en estaciones, muelles, hoteles, pensiones o casas de huéspedes.

7o. Cuando fuere de cosas religiosas o militares, de valor científico, artístico o histórico o destinadas al uso u ornato públicos.

8o. Si el hurto fuere de armas de fuego.

9o. Si el hurto fuere de ganado.

10o. Cuando los bienes hurtados fueren productos separados del suelo, máquinas, accesorios o instrumentos de trabajo, dejados en el campo, o de alambre u otros elementos de los cercos.

11o. Cuando el hurto fuere de vehículos dejados en la vía pública o en lugares de acceso público. Si los vehículos hurtados fueren llevados y aceptados en predios, talleres, estacionamientos o lugares de venta de repuestos, con destino a su venta, realización o desarme, serán solidariamente responsables con los autores del hurto, los propietarios de los negocios antes mencionados, sus gerentes, administradores o representantes legales, quienes en todo caso, están obligados a verificar la legítima procedencia de los vehículos recibidos para su comercialización. Al responsable de hurto agravado se le sancionará con prisión de 2 a 10 años".

Artículo 248. Hurto de uso. "Quien, sin la debida autorización, tomare una cosa mueble, total o parcialmente ajena, con el sólo propósito de usarla y efectuare su restitución en circunstancias que claramente lo indiquen o se dedujere de la naturaleza del hecho, dejare la cosa en condiciones y lugar que permitan su fácil y pronta recuperación, será sancionado con multa de doscientos a tres mil quetzales, sin perjuicio de las responsabilidades resultantes de los daños causados a la cosa. Cuando el hurto de uso se cometiere para efectuar plagio o secuestro o con fines o

propósitos subversivos, se impondrá al responsable prisión de dos a cinco años, sin perjuicio de las sanciones que correspondan al otro delito".

Artículo 249. Hurto de fluidos. "Quien, ilícitamente, sustrajere energía eléctrica, agua, gas, fuerza de una instalación o cualquier otro fluido ajeno, será sancionado con multas de doscientos a tres mil quetzales".

Entonces, puede inferirse por hurto a todo acto que represente la sustracción de algún elemento a una persona de manera ilegítima o sin su acuerdo o aceptación, realizado sin fuerza en las cosas, ni violencia física o intimidación en la persona, con el fin de obtener un enriquecimiento sin ningún sacrificio o esfuerzo alguno.

2.3.4 Del robo

Artículo 251. Robo. "Quien sin la debida autorización y con violencia anterior, simultánea o posterior a la aprehensión, tomare cosa, mueble total o parcialmente ajena será sancionado con prisión de 3 a 12 años".

Artículo 252. Robo agravado. "Es robo agravado:

1o. Cuando se cometiere en despoblado o en cuadrilla.

2o. Cuando se empleare violencia, en cualquier forma, para entrar al lugar del hecho.

3o. Si los delincuentes llevaren armas o narcóticos, aun cuando no hicieren uso de ellos.

4o. Si los efectuaren con simulación de autoridad o usando disfraz.

5o. Si se cometiere contra oficina bancaria, recaudatoria, industrial, comercial o mercantil u otra en que se conserven caudales o cuando la violencia se ejerciere sobre sus custodios.

6o. Cuando el delito se cometiere asaltando ferrocarril, buque, nave, aeronave, automóvil u otro vehículo.

7o. Cuando concurriere alguna de las circunstancias contenidas en los incisos 1o., 2o., 3o., 6o., 7o., 8o., 9o., 10o. y 11o. del Artículo 247 de este código. El responsable de robo agravado será sancionado con prisión de 6 a 15 años".

Artículo 253. Robo de uso. "Cuando el hecho a que se refiere el Artículo 248 de este código, se cometiere con violencia, será calificado como robo de uso y sancionado con prisión de seis a dos años. Cuando concurrieren las circunstancias a que se refiere el párrafo último del artículo citado, la pena a imponer será de tres a ocho años de prisión".

Artículo 254. Robo de fluidos. "Cuando los hechos a que se refiere el Artículo 249 de este código, se cometieren con violencia, serán calificados como robo y sancionados con prisión de seis meses a dos años".

Artículo 255. Robo impropio. "Cuando el hecho a que se refiere el Artículo 250 de este código, se cometiere con violencia, será calificado como robo impropio y sancionado con prisión de seis meses a dos años".

Respecto a los anteriores Artículos, pueden producirse estos delitos que atentan al patrimonio y que por lo tanto son muy frecuentes, a través del uso del Internet, la complejidad del asunto es cuando estos delitos se producen de un lugar dentro del territorio nacional, hacia un lugar fuera de éste, y el bien mueble regularmente que es objeto de robo, como puede ser la extracción de dinero de una tarjeta de débito o crédito, la no autorización de proporcionar el pin o contraseña para retirar dinero de

la cuenta bancaria de una persona, a una tercera persona y ésta hace mal uso de la misma, extrayendo fondos de la cuenta de la víctima, etc.

2.3.5 De la extorsión y del chantaje

Artículo 261. Extorsión. "Quien, para procurar un lucro injusto o para defraudarlo obligare a otro, con violencia, a firmar, suscribir, otorgar, destruir o entregar algún documento, a contraer una obligación o a condonarla o a renunciar a algún derecho, será sancionado con prisión de uno a seis años".

Artículo 262. Chantaje. "Comete delito de chantaje, quien exigiere a otro dinero, recompensa o efectos, bajo amenaza directa o encubierta de imputaciones contra su honor o prestigio, o de violación o divulgación de secretos, en perjuicio del mismo, de su familia o de la entidad en cuya gestión intervenga o tenga interés. El responsable de este delito será sancionado con prisión de tres a ocho años".

Puede decirse que chantaje es la presión que se hace sobre una persona, para obtener algún provecho pecuniario, material, económico u obligarla a actuar de una determinada manera, amenazándola de difamación o escándalo público o de hacer revelaciones inconvenientes, verdaderas o falsas, que afecten a su honra o a la de su familia.

Capítulo V Iniciativa de Ley de Delitos Informáticos

2.3.6 De la estafa

Artículo 263. Estafa propia. "Comete estafa quien, induciendo a error a otro, mediante ardid o engaño lo defraudare en su patrimonio en perjuicio propio o ajeno. El responsable de este delito será sancionado con prisión de seis meses a cuatro años y multa de doscientos a diez mil quetzales".

Artículo 264. Casos especiales de estafa. "Incurrirá en las sanciones señaladas en el artículo anterior:

1o. Quien defraudare a otro usando nombre fingido, atribuyéndose poder, influencia, relaciones o cualidades supuestas, aparentando bienes, comisión, empresa o negociaciones imaginarias.

2o. El platero o joyero que alterare en su calidad, ley o peso, los objetos relativos a su arte o comercio, o traficare con ellos.

3o. Los traficantes que defraudaren, usando pesas o medidas falsas, en el despacho de los objetos de su tráfico.

4o. Quien defraudare a otro con supuesta remuneración, a funcionarios, autoridades, agentes de ésta o empleados públicos, o como recompensa de su mediación para obtener una resolución favorable en un asunto que de los mismos dependa, sin perjuicio de las acciones de calumnia que a éstos corresponda.

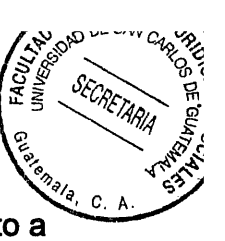
5o. Quien cometiere alguna defraudación, abusando de firma de otro, en blanco o extendiendo con ella algún documento en perjuicio del mismo o de un tercero.

6o. Quien defraudare a otro haciéndole suscribir, con engaño algún documento.

7o. Quien se valiere de fraude para asegurar la suerte en juegos de azar.

8o. Quien cometiere defraudación sustrayendo, ocultando o inutilizando, en todo o en parte, algún proceso, expediente, documento u otro escrito.

9o. Quien fingiéndose dueño de una cosa inmueble, la enajenare, gravare o dispusiere de ella, en cualquier otra forma.



10o. Quien dispusiere de un bien como libre, sabiendo que estaba gravado o sujeto a otra clase de limitaciones y quien, con su enajenación o gravamen, impidiere, con ánimo de lucro, el ejercicio de tales derechos.

11o. Quien enajena separadamente una cosa a dos o más personas, con perjuicio de cualquiera de ellas o de tercero.

12o. Quien otorgare en perjuicio de otro, un contrato simulado.

13o. Quien a sabiendas adquiriere o recibiere, en cualquier forma, bienes de quien no fuere su dueño o no tuviere derecho para disponer de ellos.

14o. Quien con perjuicio de otro, ejerciere un derecho de cualquier naturaleza a sabiendas de que ha sido privado del mismo por resolución judicial firme.

15o. Quien destruyere o deteriorare, total o parcialmente bienes que le pertenezcan, afectos a derechos de un tercero, con el propósito de defraudar a éste.

16o. Quien comprare a plazos un bien y lo enajenare posteriormente o dispusiere de él, en cualquier forma, sin haber pagado la totalidad del precio.

17o. Quien negare su firma en cualquier documento de obligación o descargo.

18o. Quien con datos falsos u ocultando antecedentes que le son conocidos, celebrare dolosamente, contratos basados en dichos datos o antecedentes.

19o. Quien sin autorización o haciendo uso indebido de ésta, mediante colectas o recaudaciones, defraudare a otros. Si la recaudación o colecta se hace sin autorización y sin propósito de defraudar, o estando autorizada no se cumple con los requisitos legales correspondientes, la sanción será de multa de veinte a doscientos quetzales.

20o. Quien cobrare sueldos no devengados, servicios o suministros no efectuados.

21o. Quien defraudare valiéndose de la inexperiencia, falta de discernimiento o pasiones de un menor o incapacitado.

22o. El deudor que dispusiere en cualquier forma, de los frutos gravados con prenda, para garantizar créditos destinados a la producción.

23o. Quien defraudare o perjudicare a otro, valiéndose de cualquier ardid o engaño, que no se haya expresado en los incisos anteriores".

Artículo 265. Estafa mediante destrucción de cosa propia. "Quien para obtener el pago de un seguro o algún provecho indebido en perjuicio de otro, destruyere, deteriorare u ocultare, total o parcialmente, un bien propio, será sancionado con prisión de uno a tres años y multa de cien a cinco mil quetzales".

Artículo 267. Estafa en la entrega de bienes. "Quien defraudare en la substancia, calidad o cantidad de los bienes que entregue a otros, en virtud de contrato o de cualquier otro título obligatorio, será sancionado con prisión de seis meses a cinco años y multa de cien a cinco mil quetzales".

Artículo 271. Estafa mediante informaciones contables. "Los auditores, contadores, expertos, directores, gerentes, liquidadores o empleados de entidad bancaria o mercantil, sociedades o cooperativas, que en sus dictámenes o comunicaciones al público, o en sus informes, memorias o proposiciones, o en la formación de los inventarios o balances, consignaren, con ánimo de defraudar, atraer inversiones o de aparentar una situación económica que no tiene, hechos contrarios a la verdad, incompletos o simulados, serán sancionados con prisión de seis meses a cinco años y multa de cien a cinco mil quetzales".

En el acto de estafa, una persona decide actuar en contra de otra violando o destruyendo su propiedad, con el objetivo de sacar un beneficio de tal situación. En este sentido, las estafas suelen ser realizadas por individuos u organizaciones delictivas que funcionan obteniendo ganancias, dinero o bienes materiales a través de la confianza o la ignorancia del perjudicado.

2.3.7 De las apropiaciones indebidas

Artículo 272. Apropiación y retención indebidas. "Quien en perjuicio de otro, se apropiare o distrajere dinero, efectos o cualquier otro bien mueble que hubiere recibido en depósito, comisión o administración, o por cualquier otra causa que produzca obligación de entregarlos o devolverlos, será sancionado con prisión de seis meses a cuatro años y multa de cien a tres mil quetzales".

Artículo 273. Apropiación irregular. "Comete el delito de apropiación irregular, quien:

1o. Tomare dinero u otro bien mueble que encontrare perdido y no le pertenezca.

2o. Habiendo encontrado un tesoro lo tomare en todo o en parte, o tomare la cuota que, según la ley, corresponda al dueño del inmueble.

3o. Tomare cosa ajena que haya llegado a su poder, por error o caso fortuito. Los responsables serán sancionados con prisión de dos meses a dos años y multa de cincuenta a dos mil quetzales".

En estos casos también resulta evidente, el perjuicio que se le puede ocasionar a los particulares con el uso del Internet, si bien es cierto, estas figuras ya están tradicionalmente reguladas en el Código Penal, no se ha establecido la complejidad con la que se cometen en el caso del Internet, y allí es en donde se considera existe perjuicio a los particulares, cuando el Estado no regula la protección a bienes jurídicos tutelados.

2.4 Legislación comparada

2.4.1 Manual de las Naciones Unidas para la Prevención y Control de los Delitos Informáticos

Este es un instrumento jurídico internacional muy importante, considerando que un buen porcentaje de naciones, forman parte de la comunidad internacional.

Este manual señala, que cuando el problema se eleva a la escena internacional, se magnifican los inconvenientes y las insuficiencias, por cuanto los delitos informáticos, constituyen una nueva forma de crimen transnacional y su combate, requiere de una eficaz operación internacional concertada.

Asimismo, la Organización de las Naciones Unidas resume de la siguiente manera, los problemas que rodean a la cooperación internacional en el área de los delitos informáticos:

"1) Falta de acuerdos globales, acerca de que tipo de conductas deben constituir delitos informáticos.

2) Ausencia de acuerdos globales, en la definición legal de dichas conductas delictivas.

3) Falta de especialización de las policías, fiscales y otros funcionarios judiciales en el campo de los delitos informáticos.

4) Falta de armonización entre las diferentes leyes procesales nacionales, acerca de la investigación de los delitos informáticos.

5) Carácter transnacional de muchos delitos cometidos, mediante el uso de computadoras.

6) Ausencia de tratados de extradición, de acuerdos de ayuda mutuos y de mecanismos sincronizados, que permitan la puesta en vigor de la cooperación internacional".

En síntesis es destacable, que la delincuencia informática se apoya en el delito instrumentado por el uso de la computadora, a través de redes telemáticas y la interconexión de la computadora, aunque no es el único medio. Las ventajas y las necesidades del flujo nacional e internacional de datos, que aumenta de modo creciente conlleva también a la posibilidad creciente de estos delitos; por eso puede señalarse que la criminalidad informática, constituye un reto considerable tanto para los sectores afectados de la infraestructura crítica de un país, como para los legisladores, las autoridades policiales encargadas de las investigaciones y los funcionarios judiciales.

"En el contexto internacional, son pocos los países que cuentan con una legislación apropiada. Entre ellos destacan, Estados Unidos, Alemania, Austria, Gran Bretaña, Holanda, Francia, España, Argentina y Chile. Dado lo anterior, a continuación se mencionan algunos aspectos relacionados con la ley en los diferentes países, así como con los delitos informáticos que persigue:

a) Estados Unidos

Este país adoptó en 1994 el Acta Federal de Abuso Computacional, que modificó al Acta de Fraude y Abuso Computacional de 1986. Con la finalidad de eliminar los argumentos híper técnicos, acerca de qué es y qué no es un virus, un gusano, un caballo de Troya y en que difieren de los virus, la nueva acta proscribe la transmisión de un programa, información, códigos o comandos que causan daños a la computadora, a los sistemas informáticos, a las redes, información, datos o programas.

La nueva ley es un adelanto, porque está directamente en contra de los actos de transmisión de virus. Asimismo, en materia de estafas electrónicas, defraudaciones y otros actos dolosos relacionados con los dispositivos de acceso a sistemas informáticos, la legislación estadounidense, sanciona con pena de prisión y multa, a la persona que defraude a otro mediante la utilización de una computadora o red informática".[12]

"En el mes de Julio del año 2000, el Senado y la Cámara de Representantes de este país, tras un año largo de deliberaciones, establece el Acta de Firmas Electrónicas en el Comercio Global y Nacional. La ley sobre la firma digital, responde a la necesidad de dar validez a documentos informáticos, mensajes electrónicos y contratos establecidos mediante Internet entre empresas (para el B2B) y entre empresas y consumidores". [13]

b) Alemania

Este país sancionó en 1986 la Ley contra la Criminalidad Económica, que contempla los siguientes delitos:

1) Espionaje de datos.

2) Estafa informática.

3) Alteración de datos.

4) Sabotaje informático.

c) Austria

[12] De la Garza, Manuel. **Estudio sobre los delitos informáticos**. Pág. 98
[13] www.goesjuridica.com.htlm. Día de consulta: 3-3-2010

"La Ley de Reforma del Código Penal sancionada el 22 de Diciembre de 1987, castiga a aquellos que con dolo causen un perjuicio patrimonial a un tercero, influyendo en el resultado de una elaboración de datos automática, a través de la confección del programa, por la introducción, cancelación o alteración de datos o por actuar sobre el curso del procesamiento de datos. Además contempla sanciones para quienes comenten este hecho, utilizando su profesión de especialistas en sistemas". [14]

d) 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 específica, la modificación de datos sin autorización.

e) Holanda

El 1º de marzo de 1993 entró en vigencia la Ley de Delitos Informáticos, en la cual se penaliza los siguientes delitos:

1) El hacking

2) El preacking (utilización de servicios de telecomunicaciones evitando el pago total o parcial de dicho servicio).

3) La ingeniería social (arte de convencer a la gente de entregar información que en circunstancias normales no entregaría).

4) La distribución de virus.

[14] www.goesjuridica.com.htlm. Día de consulta: 3-3-2010

f) Francia

En enero de 1988, este país dictó la Ley relativa al Fraude Informático, en la que se consideran aspectos como:

1) Intromisión fraudulenta que suprima o modifique datos.

2) Conducta intencional en la violación de derechos a terceros, que haya impedido o alterado, el funcionamiento de un sistema de procesamiento automatizado de datos.

3) Conducta intencional en la violación de derechos a terceros, en forma directa o indirecta, en la introducción de datos en un sistema de procesamiento automatizado o la supresión o modificación de los datos que éste contiene, o sus modos de procesamiento o de transmisión.

4) Supresión o modificación de datos contenidos en el sistema, o bien en la alteración del funcionamiento del sistema (sabotaje).

g) España

En el nuevo Código Penal de España, se establece que al que causare daños en propiedad ajena, se le aplicará pena de prisión o multa. En lo referente a:

1) Realización por cualquier medio de destrucción, alteración, inutilización o cualquier otro daño en los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos.

2) Sanciona en forma detallada esta categoría delictual (Violación de secretos/espionaje/divulgación), aplicando pena de prisión y multa.

3) En materia de estafas electrónicas, sólo tipifica las estafas con ánimo de lucro valiéndose de alguna manipulación informática, sin detallar las penas a aplicar en el caso de la comisión del delito.

h) Chile

Este país fue el primer país latinoamericano en dictar una Ley contra Delitos Informáticos, la cual entró en vigencia el 7 de Junio de 1993. Esta ley se refiere a los siguientes delitos:

1) La destrucción o inutilización de los datos contenidos dentro de una computadora, es castigada con penas de prisión. Asimismo, dentro de esas consideraciones se encuentran los virus.

2) Conducta maliciosa tendiente a la destrucción o inutilización de un sistema de tratamiento de información, de sus partes o componentes, o que dicha conducta impida, obstaculice o modifique su funcionamiento.

3) Conducta maliciosa que altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información.

2.4.2 Convención Europea sobre el ciber crimen

Dentro de los aspectos más importantes de resaltar de este instrumento, se encuentran los siguientes:

Establece que los Estados miembros del Consejo de Europa y los demás Estados signatarios del presente convenio, teniendo en cuenta que el objetivo del Consejo de Europa, es lograr una mayor unidad entre sus miembros; reconociendo la importancia de fomentar la cooperación con los demás Estados partícipes en la presente convención; convencida de la necesidad de llevar a cabo, como cuestión de

prioridad, una política penal común encaminada a la protección de la sociedad contra el delito cibernético, entre otras cosas, mediante la adopción de una legislación adecuada y el fomento de la cooperación internacional

Además, de que consciente de los profundos cambios provocados por la digitalización, la convergencia y la continua globalización de las redes informáticas; preocupado por el riesgo de que las redes de computadoras y electrónicos de información, también pueden ser utilizados para cometer delitos y que las pruebas relativas a esos delitos, pueden ser almacenadas y transferidas por estas redes.

Reconociendo la necesidad de la cooperación entre los Estados y la industria privada, en la lucha contra la delincuencia cibernética y la necesidad de proteger, los intereses legítimos en el uso y desarrollo de tecnologías de la información.

Estimando que una lucha eficaz contra los delitos informáticos, requiere un aumento, rápido y el buen funcionamiento de la cooperación internacional en materia penal.

Convencido de que el presente convenio es necesario, para disuadir la acción dirigida contra la confidencialidad, integridad y disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el uso indebido de tales sistemas, redes y datos mediante el establecimiento de la penalización de esa conducta, como se describe en el presente convenio; y la adopción de poderes suficientes para luchar eficazmente contra esos delitos, facilitando su detección, la investigación y el enjuiciamiento, tanto a nivel nacional e internacional y por la adopción de disposiciones, para la cooperación internacional rápida y fiable de la operación.

Consciente de la necesidad de garantizar un equilibrio adecuado, entre los intereses de aplicación de la ley y el respeto de los derechos humanos fundamentales consagrados en la década de 1950 del Consejo de Europa, Convenio para la Protección de los Derechos Humanos y las Libertades Fundamentales de 1966 de las Naciones Unidas, Pacto Internacional de Derechos Civiles y Políticos y otros

instrumentos internacionales aplicables de derechos humanos, donde se reafirma el derecho de toda persona a tener opiniones sin interferencias, así como el derecho a la libertad de expresión, incluida la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, y los derechos sobre el respeto de la intimidad.

Consciente también del derecho a la protección de los datos personales que le otorga, por ejemplo, la de 1981 del Consejo de Europa, Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos Personales.

Teniendo en cuenta la Convención de las Naciones Unidas de 1989, sobre los Derechos del Niño y la de 1999, de la Organización Internacional del Trabajo sobre las peores formas de trabajo infantil.

Tomando en cuenta los Convenios sobre la Cooperación en el Ámbito Penal, así como los tratados similares que existen entre los Estados miembros del Consejo de Europa y otros Estados, y subrayando que el presente convenio, tiene por objeto complementar otros convenios, con el fin de realizar investigaciones y actuaciones penales, concernientes a delitos con sistemas y datos informáticos, y para que la recolecta de pruebas en formato electrónico de un delito penal sea eficaz.

Acogiendo con beneplácito los recientes acontecimientos, que el avance del entendimiento internacional y la cooperación en la lucha contra la ciber delincuencia, incluidas las medidas adoptadas por las Naciones Unidas, la OCDE, la Unión Europea y el G8.

Recordando las recomendaciones del Comité de Ministros No. R (85) 10, sobre la aplicación práctica del Convenio Europeo de Asistencia Judicial en Materia Penal, en Materia de Comisiones Rogatorias para la Interceptación de las Telecomunicaciones No. R (88) 2, sobre la Piratería en el Ámbito de los Derechos de Autor y derechos conexos No. R (87) 15, que regula el uso de datos personales en el sector de la

policía No. R (95) 4, sobre la Protección de Datos Personales en el Ámbito de los Servicios de Telecomunicaciones, con especial referencia a los servicios de teléfono No. R (89) 9, en el ordenador proporcionar a los legisladores nacionales la definición de algunos delitos informáticos, y No. R (95) 13 relativa a los problemas de Derecho Procesal Penal relacionados con la tecnología de la información.

Vista la Resolución No. 1 adoptada por los Ministros de Justicia Europeo en su 21º Conferencia (Praga, 10 y 11 de Junio de 1997), que recomendó al Comité de Ministros, apoyar el trabajo sobre los delitos informáticos realizados por el Comité Europeo para Problemas Criminales (CDPC) y permitir el uso de medios efectivos de investigación de esos delitos, así como la Resolución No. 3 aprobada en la 23º Conferencia de los Ministros de Justicia Europeo (Londres, 8 y el 9 de Junio de 2000), que alienta a las partes negociadoras, a proseguir sus esfuerzos con miras a encontrar soluciones adecuadas para que el mayor número posible de Estados se adhieran a la Convención y reconoció, la necesidad de un sistema rápido y eficaz de la cooperación internacional, cooperación que tiene debidamente en cuenta las necesidades específicas de la lucha contra la delincuencia informática;

Teniendo también en cuenta el Plan de Acción aprobado por los Jefes de Estado y de Gobierno del Consejo de Europa en el momento de su Segunda Cumbre (Estrasburgo, 10 y 11 de Octubre de 1997), para buscar respuestas comunes al desarrollo de las nuevas tecnologías de información basados en las normas y valores del Consejo de Europa.

El Artículo 1 se refiere a las definiciones, y por considerarlas importantes, se señalan a continuación:

"a) Un sistema informático es: Cualquier producto o grupo de aparatos interconectados o relacionados, de conformidad con un programa o el tratamiento automático de datos.

b) Datos informáticos: Toda representación de hechos, informaciones o conceptos de una forma adecuada, para su transformación en un sistema informático.

c) Prestador de servicios significa: Cualquier entidad pública o privada, que proporciona a los usuarios de sus servicios, la posibilidad de comunicarse por medio de un sistema informático, y cualquier otra entidad que procesa o almacena datos de la computadora, en nombre del servicio de comunicación o los usuarios de dicho servicio.

d) Datos de tráfico: Cualesquiera datos informáticos relativos a una comunicación por medio de un sistema informático, generados por un sistema informático que formaba parte de la cadena de comunicación, con indicación del origen de la comunicación, destino, ruta, hora, fecha, tamaño, la duración o el tipo de servicio subyacente".

CAPÍTULO III

3. La iniciativa de Ley de Delitos Informáticos, los conflictos de jurisdicción que se generan y la necesidad de que entre en vigencia en el ordenamiento jurídico guatemalteco

3.1 Aspectos considerativos

Como se ha podido observar, en la actualidad las computadoras se utilizan no sólo como herramientas auxiliares de apoyo a diferentes actividades humanas, sino además como medio eficaz para obtener y conseguir información, lo que las ubica también como un nuevo medio de comunicación, y condiciona su desarrollo a la informática; tecnología cuya esencia se resume en la creación, procesamiento, almacenamiento y transmisión de datos.

A la par de ello, evidentemente por las bondades que ofrecen estas herramientas, han sido motivaciones suficientes para los criminales y en este caso, los de alta jerarquía cultural y educativamente hablando, para cometer ilícitos, como los que se han señalado en el transcurso de este trabajo.

Aquí se está entonces ante un problema mayor para el Estado, como garantizador del bienestar social y de la protección a los bienes jurídicos, ya tutelados en la ley penal y que se cometen frecuentemente, pero utilizando como herramienta no precisamente las formas tradicionales, sino la herramienta del Internet y las computadoras.

Es por ello que aparte de que en este trabajo, se hace una descripción de las figuras delictivas consideradas como delitos informáticos, también es que debe el Estado regular aspectos fundamentales, pero desde el punto de vista del quebrantamiento de los sistemas de control de origen, en el caso de los delitos que se cometen por el uso del Internet y no precisamente, como se regula en el Código Penal, refiriéndose

a figuras delictivas generalizadas y tradicionales, dejando por un lado y bajo un estado de impunidad, las que se han señalado y que más adelante se refiere el autor con mayor detalle.

3.2 Análisis de la iniciativa de ley

Esta iniciativa ha tenido como motivación lo siguiente:

De conformidad con la Constitución Política de la República de Guatemala, es obligación del Estado brindar seguridad o certeza jurídica. En ese sentido, debe entenderse que como parte de esa obligación de seguridad, el Estado de Guatemala, debe brindar y garantizar los mecanismos necesarios, para regular la conducta de sus habitantes y, proteger y sancionar los actos o abusos que se cometan en cualquier ámbito social.

La presente iniciativa se refiere, a normas especiales para proteger y sancionar todos aquellos ilícitos de naturaleza informática, que sean cometidos en Guatemala o que surtan efectos jurídicos en su territorio.

El bien jurídico tutelado, según las disposiciones de la presente iniciativa, lo constituye la información. La información como tal y bajo el tratamiento de la presente iniciativa, es un bien jurídico tutelado de índole novedosa, que como política criminal debe ser tratado, a través de una ley especial y no mediante reforma, adición o derogatoria de normas del actual Código Penal.

En la presente iniciativa, se pretende sancionar penalmente por delitos informáticos y establecer un marco regulatorio, sobre posibles usos indebidos que perjudican transacciones y el comercio electrónico. Esta ley contempla, las definiciones legales propias para el tema del ciber crimen y desarrolla la normativa pertinente para sancionar entre otros, los actos de hacking (acceso sin autorización), craking (daño o sabotaje), phishing, smishing, vishing (invitación de acceso a sitios o sistemas

informáticos falsos o fraudulentos) y pornografía infantil entre otros ilícitos informáticos.

Se busca imponer sanciones drásticas, a los responsables de los ilícitos aquí tipificados y que refieren fraude informático, pornografía infantil, acceso ilícito mediante interceptación, interferencia o utilización de sistemas o datos informáticos, daño informático, posesión de equipos o prestación de servicios para daño informático, espionaje informático, falsificación informática e invitación de acceso a sitios o sistemas informáticos falsos o fraudulentos.

Además, se pretende la creación de una unidad de especialización, para la investigación criminal de estos delitos.

También tiene como fundamento, la necesaria y efectiva creación y aplicación de normas especiales, toda vez que por la naturaleza de los actos de ciber crimen, se complica la aplicación de las actuales normas del Código Penal, por lo que se traduce en lagunas legales, que permiten al delincuente realizar actos ilícitos por medio de las nuevas tecnologías de la información.

Dentro del contenido es importante resaltar lo siguiente:

El Artículo 1 se refiere al objeto de la ley, y preceptúa: "Tiene por objeto dictar medidas de prevención y sanción de los actos ilícitos de naturaleza informática, cometidos a través de artificios tecnológicos, mensajes de datos, sistemas o datos informáticos. Así como medidas de protección contra la explotación, la pornografía infantil, y demás formas de abuso sexual contra menores de edad y que se realicen por medio de sistemas informáticos".

El Artículo 2 se refiere a las definiciones que en materia informática, "se manejan a través de esta ley, siendo necesario por cuanto debe entenderse, como se pueden interpretar las conductas realizadas por los delincuentes especiales en este ámbito".

Debido a que las denominaciones que se utilizan son en idioma inglés, no cabe duda que las conductas para el caso deben ser traducidas al español, y como todavía no se han definido, se hace necesario conocer ciertos conceptos:

a) Datos informáticos: Toda representación de hechos, instrucciones, caracteres, información o conceptos, expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función.

b) Documento: Registro incorporado en un sistema en forma de escrito, video, audio o cualquier otro medio que contiene información acerca de un hecho o acto capaces de causar efectos jurídicos.

c) Pornografía infantil: Toda representación de un menor de edad, dedicado a actividades explícitas reales o simuladas de carácter sexual, realizadas a través de escritos, objetos, medios audiovisuales, electrónicos, sistemas de cómputo, o cualquier medio que pueda utilizarse para la comunicación y que tienda a excitar sexualmente a terceros, cuando esta representación no tenga valor artístico, literario, científico, o pedagógico.

d) Sistema informático: Dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre si, cuya función o la de alguno de sus elementos, sea el tratamiento automatizado de datos, en ejecución de un programa entre los cuales se encuentran los programas, sitios o páginas de Internet.

e) Tarjeta inteligente: Instrumento de identificación, de acceso a un sistema de pago o de crédito, y que contiene datos o información de uso restringido.

f) Tecnología de información: Rama de la tecnología que se dedica al estudio aplicación y procesamiento de información, lo cual involucra la obtención, creación, almacenamiento, administración, modificación, manejo, movimiento, control,

visualización, distribución, intercambio, transmisión, o recepción de información, en forma automática, así como el desarrollo y uso de equipos y programas, cualesquiera de sus componentes y todos los procedimientos, vinculados con el procesamiento de la información.

Como algo fundamental dentro del enfoque de este trabajo, se encuentra lo contenido en el Artículo 3 de la iniciativa objeto de análisis, por cuanto delimita el ámbito de aplicación de dicha ley, y que señala: "La presente ley será aplicable a los responsables de hechos punibles, si estos hubieren sido cometidos en la República de Guatemala. Cuando alguno de los delitos previstos en la presente ley, se cometa fuera del territorio de la República, el responsable quedará sujeto a sus disposiciones, si dentro del territorio de la República, se hubiere producido efectos del hecho punible, y el responsable no ha sido juzgado por el mismo hecho o ha evadido el juzgamiento o la condena por tribunales extranjeros".

Al referirse la ley a los delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos, señala los siguientes:

a) Acceso sin autorización. "El que sin plena autorización acceda, intercepte, interfiera o utilice un sistema o dato informático, de naturaleza privada o pública, y de acceso restringido será penado con prisión de dos a seis años".

b) Daño informático: "El que ilegítimamente alterare, destruyere, inutilizare, suprimiere, modificare, o de cualquier modo o de cualquier medio dañare un sistema o dato informático, será penado con prisión de cuatro a ocho años".

c) Posesión de equipos o prestación de servicios para daño informático: "El que con el propósito de destinarlos a alterar, destruir, inutilizar, suprimir, modificar o dañar, un sistema o dato informático, posea, fabrique, importe, distribuya, comercialice, o utilice equipos o dispositivos, o el que ofrezca, preste servicios, destinados a cumplir los mismos fines, será penado con prisión de tres a seis años".

d) Espionaje informático: "El que ilegítimamente se apoderare, obtenga, revele, transmita o difunda el contenido parcial o total de un sistema o dato informático, de carácter público o privado, será penado con prisión de cuatro a ocho años".

En el caso de los delitos informáticos, relacionados con la propiedad y autenticidad, señala los siguientes:

a) Fraude informático: "El que para obtener algún beneficio, para si o para un tercero, mediante cualquier artificio tecnológico, o manipulación de un sistema o dato informático, procure la transferencia no consentida, de cualquier activo patrimonial en perjuicio de otro, será penado con prisión de tres a ocho años".

b) Uso fraudulento de tarjeta inteligente o instrumentos análogos: "Quien de manera deliberada o ilegítima, cree, utilice, capture, grabe, copie, altere, duplique o elimine, el contenido de una tarjeta inteligente, o cualquier instrumento destinado a los mismos fines, cause un perjuicio económico, al legítimo usuario o a cualquier persona será penado con prisión de tres a siete años".

c) Provisión indebida de bienes o servicios: "Quien a sabiendas de que una tarjeta inteligente, o instrumento destinado a los mismos fines, han sido falsificados, alterados, se encuentran vencidos o revocados o han sido indebidamente obtenidos, provea a quien los presente de dinero, efectos, bienes o servicios, será penado con prisión de uno a cinco años".

d) Posesión de equipo para falsificaciones: "Quien sin estar debidamente autorizado para emitir, fabricar, o distribuir tarjetas inteligentes o instrumentos análogos, posea, importe, reciba, adquiera, transfiera, comercialice, controle o custodie, cualquier equipo de fabricación de tarjetas inteligentes o de instrumentos destinados a los mismos fines, o cualquier equipo o componente que capture, grabe, copie, o transmita el contenido de dichas tarjetas o instrumentos, será penado con prisión de dos a seis años".

e) Falsificación informática: "Quien a través de cualquier medio, cree, altere, modifique o elimine total o parcialmente, un sistema, documento o dato informático y simule su autenticidad, será penado con prisión de dos a seis años; igual pena se aplicará para el que por cualquier medio, conduzca, enlace o remita a un sitio o sistema informático falso o fraudulento, la pena será de cuatro a ocho años de prisión, cuando las conductas a que se refieren los párrafos anteriores sean cometidas para procurar un beneficio propio o ajeno".

f) Invitación de acceso: "El que de manera deliberada, e ilegítima, a través de mensaje de datos, o de cualquier otro medio, atraiga o invite a ingresar a un sitio o sistema informático falso o fraudulento, será sancionado con prisión de uno a cinco años. La pena será de dos a seis años de prisión, cuando las conductas a que se refiere el párrafo anterior, sean cometidas para procurar un beneficio propio o ajeno".

Respecto a los delitos contenidos en esta ley, que se relacionan con contenido, se indica al delito de pornografía infantil y establece:

"Quien a través de un sistema informático, mensaje de datos o por cualquier medio que involucre el uso de tecnologías de información, difunda, transmita, ofrezca, o comercialice utilizando la imagen o sonidos que provengan de un menor de edad, o de una persona que parezca un menor, con fines exhibicionistas o pornográficos, será sancionado con prisión de seis a doce años inconmutables, y con una multa de cien mil a novecientos mil quetzales". En este caso, no se podrá otorgar cualquiera de las medidas sustitutivas contempladas en el Código Procesal Penal.

Igual pena se aplicará para el que fabrique, importe o exporte, material pornográfico, utilizando la imagen o sonidos que provengan de un menor o de una persona que parezca un menor. Cuando las conductas a las que se refiere el párrafo anterior, se realicen por medio de dibujos de menores de edad, la pena de prisión será de uno a cinco años.

También se regula en el apartado anterior, el delito de alteración de imágenes que dice: "Quien de manera deliberada o ilegitima a través de mensaje de datos o cualquier otro medio envíe, transmita o aloje, en sistemas informáticos, imágenes, o fotografía de personas, con fines exhibicionistas o pornográficos, será sancionado con prisión de tres a seis años y multa de diez mil a cien mil quetzales. Igual pena se aplicará para quien modifique, altere imágenes o fotografías de personas con fines exhibicionistas, o pornográficos, que menoscaben la dignidad de la persona".

Se refiere también la ley, a la creación de la Unidad de Investigación especializada en Delitos Informáticos, otorgando el plazo de 60 días para crearla por parte del Ministerio Público.

Como se observa es evidente que con esta iniciativa, se pretende dar un paso positivo en el tema de los nuevos ilícitos, que han ido apareciendo con relación al uso del Internet, los perjuicios que se ocasionan a terceros, el interés de la comunidad internacional, como sucede en el caso de la Convención Europea contra el Ciber crimen, respecto a la jurisdicción y competencia de los mismos, sin embargo, como se evidencia en el desarrollo de todo el trabajo, hacen falta muchos de los ilícitos que pueden cometerse con relación a estas prácticas, de lo cual se propone más adelante para que ésta se mejore.

3.3 Los nuevos ilícitos y los conflictos de jurisdicción

Pese a estos y otros esfuerzos, las autoridades aún afrentan graves problemas en materia de informática. El principal de ellos, es la facilidad con que se traspasan las fronteras, por lo que la investigación, enjuiciamiento y condena de los transgresores, se convierte en un dolor de cabeza jurisdiccional y jurídico.

Además, una vez capturados tienen que escoger, entre extraditarlos para que se les siga juicio en otro lugar, o transferir las pruebas al lugar donde se cometieron los delitos.

"En 1992, los piratas de un país europeo atacaron un centro de computadoras de California. La investigación policial se vio obstaculizada, por la doble tipificación penal, la carencia de leyes similares en los dos países, que prohibían ese comportamiento. Esto impidió la cooperación oficial, según informa el Departamento de Justicia de los Estados Unidos. Con el tiempo la policía del país de los piratas, se ofreció a ayudar, pero poco después la piratería terminó, se perdió el rastro y se cerró el caso.

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

Los oficiales del país sudamericano, requisaron el apartamento del pirata e incautaron su equipo de computadora, aduciendo posibles violaciones de las leyes nacionales. Sin embargo, los dos países no habían firmado acuerdos de extradición por delitos de informática, sino por delitos de carácter más tradicional.

Finalmente se resolvió la situación, sólo porque el pirata accedió a negociar su caso, lo que condujo a que se declarara culpable en los Estados Unidos. Las dificultades que enfrentan las autoridades en todo el mundo, ponen de manifiesto la necesidad apremiante de una cooperación mundial, para modernizar las leyes nacionales, las técnicas de investigación, la asesoría jurídica y las leyes de extradición para poder alcanzar a los delincuentes. Ya se han iniciado algunos esfuerzos al respecto".[15]

[15] www.goesjuridica.com.htlm. Acalma Santos, Luis. **Problemas que se enfrenta por los conflictos de jurisdicción en el tema de los delitos informáticos.** Día de consulta: 3-3-2010.

3.4 La realidad actual

Los ilícitos penales que se cometen a través de Internet poseen algunas particularidades: La falta de una tipificación específica en la mayoría de las legislaciones de los delitos cometidos a través de la red; la transnacionalidad de las conductas, que muchas veces se realizan en un país, pero cuyos resultados se producen en otro; la falta de consenso internacional sobre la reprochabilidad de ciertas conductas; la virtualidad de estas conductas; las permanentes innovaciones tecnológicas que, generalmente avanzan más rápido que las implementaciones de soluciones normativas. Asimismo, los delitos cometidos por Internet presentan innumerables dificultades en su persecución, ya que es difícil detectar los delitos cometidos y localizar a quien los comete.

En efecto el llamado ciber crimen, presenta la dificultad de que la mayoría de los casos y conductas que los generan son multinacionales, lo que choca con las soluciones territoriales de los sistemas jurídicos nacionales, siendo un ámbito propicio para el fraude y los paraísos informáticos. De ahí la importancia de la sanción de convenciones internacionales y la adopción de parámetros comunes internacionales.

El problema de la competencia en los delitos informáticos transnacionales, es uno de los mayores inconvenientes que presentan los delitos informáticos, en cuanto a la frecuente extraterritorialidad que traen aparejados, ya que los delitos pueden ser cometidos, por una persona que se encuentra físicamente en un país y los efectos pueden producirse en otro, instalando interrogantes sobre el tribunal competente para juzgar dichos delitos.

Es así, como siendo motivo de investigación en el presente estudio, se encuentran dos posibles posturas: considerar competente al tribunal del país en el cual se produjo el daño, o confirmar la competencia del país en el cual se encuentra el autor

del delito. Esta determinación es fundamental, ya que el tribunal competente va a resolver el caso aplicando su propia legislación penal.

Este problema ha sido tratado por los tribunales norteamericanos, prevaleciendo el criterio de considerar el lugar donde se producen los efectos del hecho ilícito, como atributivo de competencia.

Ahora bien, es menester señalar que el criterio antes abordado, no es el único que se aplica en la materia, ya que si se encuentra frente al caso de un virus, que se origina en un determinado lugar y expande sus efectos sobre varios países, se generará el inconveniente de la concurrencia de jurisdicciones, que se consideran competentes para juzgar el hecho.

En tales casos para evitar la necesidad de realizar interpretaciones, verbigracia sobre la jurisdicción, en el cual se produjo el mayor daño y que sería competente para juzgar el hecho, o ante la necesidad de seleccionar un requerimiento de extradición del presunto delincuente, entre todos los países que la solicitan es conveniente que sea competente la jurisdicción del autor del hecho, aunque correlativamente los países que no penalizan al delito informático, pueden ser considerados como paraísos informáticos, para perpetrar este tipo de delitos.

En conclusión, el principio arribado por los tribunales en forma generalizada es, que una persona puede ser juzgada en el lugar en el cual el daño fue provocado, a pesar de no encontrarse en dicha jurisdicción, cuando comenzaron los actos que resultaron en dicho daño. Este criterio tiene la ventaja, de permitir la sanción de conductas que podrían no ser sancionadas, pero su aplicación práctica requiere de una gran colaboración entre los Estados y facilidades para la extradición de los delincuentes.

Por lo tanto, en ciertas situaciones puede ser práctica la aplicación del criterio, de juzgar el delito en el lugar en el cual reside el autor del hecho, pero dicha situación no debe ser utilizada, para que este tipo de delitos queden impunes.

3.5 La solución contenida en la ley

Es de hacer notar que no existe claridad en las legislaciones, y mucho menos en el caso de Guatemala, respecto a la jurisdicción y competencia en este tipo de ilícitos, especialmente por las características sui generis de los mismos.

Por otro lado, la Ley de Delitos Informáticos que se analiza, y que actualmente se encuentra en iniciativa, en el Artículo 3 señala: "La presente ley será aplicable a los responsables de los hechos punibles, si éstos hubieren sido cometidos en la República de Guatemala. Cuando alguno de los delitos previstos en la presente ley, se cometen fuera del territorio de la República, el responsable quedará sujeto a las disposiciones si dentro del territorio de la República, se hubieren producido efectos del hecho punible, y el responsable no ha sido juzgado, por el mismo hecho o ha evadido el juzgamiento, o la condena por tribunales extranjeros".

Como se observa, se conservan los principios fundamentales en esta materia, que se señalan en la Convención Contra el Ciber Crimen, en lo que respecta a los delitos informáticos y en lo relativo a la jurisdicción y competencia, es conveniente establecer lo siguiente:

Como se mencionó anteriormente, la Convención de Ciber delitos del Consejo de Europa, tiene principalmente dos objetivos: la introducción de conductas tipificadas con términos similares y la coordinación y cooperación entre las policías y administraciones de los países que se adhieran a ella. Dentro de dicho contexto, en el Capítulo II del Convenio se establecen una serie de medidas, que deben tomarse a nivel nacional para castigar ciertos delitos informáticos. El mencionado Convenio, tiene la particularidad de traer normas de derecho material y de derecho procesal.

Dentro de las disposiciones de derecho sustancial, los delitos informáticos son clasificados en la Convención en cuatro grupos:

"a) Delitos contra la confidencialidad, la integridad y la disponibilidad de datos y sistemas informáticos.

b) Delitos relacionados con el uso de computadoras.

c) Delitos relacionados con los contenidos.

d) Delitos relacionados con la violación del derecho de autor y otros derechos relacionados".

La comisión de todos los tipos previstos por el convenio, deben ser penados por los Estados miembros, no sólo con relación al autor del mismo, sino también se debe castigar su ayuda y su instigación. El castigo de dichos delitos, se debe realizar mediante sanciones efectivas, proporcionales y disuasivas, que pueden llegar a incluir la privación de la libertad.

Asimismo, se estipula la posible responsabilidad de las personas jurídicas, para su beneficio y cometido por cualquier persona física, que actúe individualmente o como parte de un órgano de la persona jurídica, que tenga una posición importante en virtud de un poder de representación de la persona jurídica, facultades para tomar decisiones, en nombre de la persona jurídica o facultades para ejercer controles dentro de la persona jurídica.

La responsabilidad puede ser civil, administrativa o penal, sin perjuicio de la responsabilidad penal que corresponda a las personas físicas, que cometieron el delito. En este caso, las sanciones eficaces serán de carácter penal o no, incluyendo sanciones monetarias. Además, el convenio prevé una serie de remedios procesales, para hacer efectivos los derechos de las personas y castigar los delitos penales establecidos en éste, otros cometidos a través de un sistema informático y la recopilación de pruebas en formato electrónico de un delito penal.

Dentro de las medidas procesales previstas se encuentran:

a) La pronta preservación de los datos informáticos almacenados.

b) La orden de suministrar.

c) El allanamiento del lugar donde se encuentren y secuestrar datos informáticos almacenados.

d) La recopilación de datos informáticos en tiempo real.

e) La interceptación de datos de contenidos.

Orden de suministrar. Este remedio procesal, permite ordenar a una persona que se encuentre dentro del territorio del país, que suministre datos informáticos específicos que dicha persona posea o controle, o a un proveedor que ofrezca servicios informáticos en el territorio para que informe sobre sus abonados. Dicha información sobre los abonados, debe permitir establecer el tipo, técnicas y períodos de servicio; la identidad del abonado, el número de acceso e información relacionada con la facturación; o cualquier información que se pueda obtener relacionada con la instalación de equipos de comunicaciones.

En cuanto a la jurisdicción, se adoptan una serie de principios atributivos de la misma: Si el delito es cometido dentro del territorio del Estado; si el delito se comete a bordo de un barco de su bandera; si el mismo se comete a bordo de una aeronave registrada en virtud de leyes de esa parte; o si el delito es cometido por uno de sus ciudadanos y el mismo es punible en el lugar donde se cometió, o si es cometido fuera de la jurisdicción de cualquier Estado.

Por ende, la Convención adopta básicamente los principios de territorialidad y nacionalidad, para atribuir jurisdicción en este tipo de delitos. Cabe destacar, que en

el caso que más de un Estado, reclame tener jurisdicción sobre un presunto delito, las partes deberán efectuar consultas, para determinar la jurisdicción más apropiada donde llevar a cabo el procedimiento penal, tratando de evitar eventuales conflictos de jurisdicción entre los Estados y armonizar los dos principios adoptados.

También esta Convención dispone un capítulo sobre cooperación internacional, extradición y asistencia mutua, para poder sancionar los delitos cometidos por medios informáticos, teniendo en cuenta la gran extraterritorialidad que presenta la materia.

Como se evidencia, la Convención regula de manera más directa y detallada, todos los aspectos que deben contemplarse, derivados del lugar en donde se producen los efectos del delito y de todas las circunstancias, que puedan proveerse en relación a evitar la impunidad de los mismos, por lo que esta deficiencia se encuentra en la legislación nacional.

Así también, regula una serie de ilícitos que han sido previstos, precisamente por el hecho de que los mismos, se han dado en la realidad y que por esa razón, deben contemplarse en las legislaciones de los Estados parte.


FACULTAD DE CIENCIAS JURIDICAS Y SOCIALES
UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
SECRETARIA
Guatemala, C. A.

CAPÍTULO IV

4. Ventajas de que entre en vigencia la Ley de Delitos Informáticos y las propuestas de solución a la problemática de competencia y jurisdicción

4.1 Antecedentes

Se acepta en forma genérica que la jurisdicción, es la facultad que tiene el Estado para administrar justicia en un caso concreto, por medio de los órganos judiciales instituidos al efecto, para cumplir dicha finalidad, se sostiene que la función reúne al menos los siguientes elementos, a saber: Notio: Facultad para compeler a las partes al proceso; Coertio: Facultad para emplear la fuerza pública para el cumplimiento de lo ordenado en el proceso; Judicium: Facultad de resolver el conflicto con carácter definitivo; y Executio: Facultad de ejecutar lo dispuesto, incluso mediante la fuerza pública de ser necesario.

La competencia en cambio, es la atribución legítima a un juez u otra autoridad para el conocimiento o resolución de un asunto. Transnacionalidad o transterritorialidad, de los actos dañosos que esta nueva tecnología implica. Es cierto que como primera medida, debe siempre tenerse en cuenta esta transnacionalidad, a fin de realizar una aproximación coherente, a las conductas de los posibles transgresores de los derechos ajenos.

Esta extraterritorialidad de los actos lesivos y la dificultad de encuadramiento personal de los sujetos activos, presenta un cuadro difícil de resolver en la mayoría de las situaciones prácticas, a lo que debe agregarse la casi imposibilidad de identificar a los transgresores en forma fehaciente, durante sus actividades en la red.

Es un principio generalmente aceptado la territorialidad estricta del derecho penal, lo cual refleja en realidad el principio de juez natural, reconocido en los Tratados

Internacionales de Derechos Humanos, pero como todo principio éste admite algunas excepciones.

"Dentro de estas excepciones, se puede señalar aquella que permite la extraterritorialidad del derecho penal, en aquellos casos en que los efectos del delito, se produzcan dentro del territorio que se arroga la aplicación de su derecho o la que implica, que se hace extensiva la aplicación del derecho penal de un Estado, cuando los efectos del delito afecten en forma directa los intereses del mismo.

Como sucede con lo regulado en el Artículo 3 de la Ley de Delitos Informáticos que se encuentra como iniciativa actualmente y la Convención Europea sobre el Ciber Crimen, estos dos casos son recogidos por casi todos los ordenamientos del mundo, como ejemplo de la extraterritorialidad de la aplicación del derecho penal. Según estos principios, se puede decir que en casi todos los casos, resultaría aplicable la ley penal del lugar donde se produzcan los efectos del delito".

Pero claro, regresando al problema planteado en un inicio, en los delitos informáticos se puede decir que, es donde se producen los efectos. En el lugar donde se asienta el servidor que sostiene la página, o donde el damnificado por las violaciones de propiedad intelectual, pierde en forma ilegítima sus derechos, o su intimidad, o sufre un menoscabo en su patrimonio, por ejemplo.

Cualquiera de las dos opciones parece razonable, pero si debe tomarse en cuenta que siempre, en forma anexa a la demanda penal por violación de propiedad intelectual, violación de intimidad o detrimento patrimonial por ejemplo, que se tratare de estos ilícitos en el Internet, existe un reclamo por vía civil, principalmente la afectación en el patrimonio que dichos actos o hechos conlleva, por lo que sería lo más lógico, que independientemente de en que locación o territorio, se encuentre asentado el servidor que soporta la página Web o la base de datos que es objeto del delito, corresponde la aplicación de las leyes del territorio en el cual el sujeto pasivo,

ve menoscabados sus derechos patrimoniales y/o morales, toda vez que la protección de estos derechos, son en definitiva los bienes jurídicos protegidos.

El único inconveniente se puede plantear, en los casos en que los daños se produjeren en forma simultánea en varios Estados, para lo cual se pueden tener soluciones alternativas y que deben estar previamente reguladas por el principio de legalidad, como por ejemplo, el hecho de que corresponda la aplicación de la ley del país o Estado en que el delito fuere más grave, aunque en verdad y prima facie, pueda decirse que esto entraría en conflicto con el principio de ley penal más benigna, cosa que no es así desde que éste, hace referencia a las leyes de un mismo ordenamiento, y no sucede en casos como el planteado.

Para aquellos casos, en que se habla de delitos o daños de igual magnitud (ya que la entidad de los daños causados, puede ser asimismo un criterio de aplicabilidad de la ley), se puede decir que, correspondería por ejemplo a la ley propia del país es decir aquel Estado que hubiese iniciado las actuaciones primero, y en caso de persistir, aún queda el criterio de que corresponde la aplicación de la ley del lugar en que el sujeto activo fuere detenido, con lo cual siempre se encontraría en diversos rangos, una solución para evitar la superposición de dos o más ordenamientos aplicables.

A) La competencia jurisdiccional

Una vez resuelto el problema de la ley aplicable, corresponde al ordenamiento interno de cada país, según las normas de derecho penal internacional o interno, la determinación del juez competente en cada caso en particular, pero con la salvedad de que en caso, de no estar ésta determinada por el ordenamiento interno, debe siempre sujetarse a los jueces de competencia, según se denomine en cada caso o bien del fuero común, si así se determinare.

B) La extradición

Constituye una salida jurídica, ante el problema de la imputación a los sujetos activos de este tipo de delitos, y favorece también la cooperación internacional de los Estados. La misma implica la interacción de al menos dos estados y ello, supone algunas condiciones de coincidencia mínimas entre ambos ordenamientos, como factores previos y determinantes para que proceda.

Aparte de lo anterior, una de las coincidencias mínimas para que se aplique, es la que se funda en el hecho de que el acto perseguido, debe ser delito en ambas jurisdicciones, lo cual a la altura del desarrollo del derecho penal informático, que hoy encuentra en la práctica un obstáculo casi infranqueable, ya que la mayoría de los delitos electrónicos o informáticos, no se encuentran legislados casi en ningún país del mundo, lo cual implica una casi imposibilidad fáctica de la misma.

Por otra parte debe tenerse en cuenta también, el hecho de que si se trata de delitos menores, o como sea que la legislación interna denomine, a los que poseen penas privativas de la libertad menores a dos o tres años según el caso, por ejemplo, los mismos resultan para casi todas las legislaciones como no extraditables, razón que impone una nueva restricción a los casos que nos ocupan, si esto no se prevé en forma adecuada al momento de realizar la legislación de cada Estado.

A poco que se medite la solución es casi única, establecer un tratado internacional específico, para regular las cuestiones planteadas, y por sobre todo la extradición, pero con el claro inconveniente, de que cualquier país o grupo de países que no firmen y ratifiquen el tratado, de hecho ponen en peligro en forma directa la efectividad del mismo, toda vez que cuando los sujetos activos se encuentren en su territorio, resultará imposible la extradición de los mismos para su juzgamiento.

Como solución alternativa hasta tanto se logre un marco internacional adecuado, podría preverse que la investigación de los hechos y la captura de los sujetos

involucrados, quede a cargo de la INTERPOL por ejemplo, dado su carácter transnacional u de otro organismo similar, que pueda cumplir sus funciones en la mayoría de los Estados, posiblemente afectados por conductas de los tipos descriptos en el presente trabajo.

Como última consideración, pero no por ello menos importante, debe también tenerse en cuenta el hecho, de que casi la totalidad de los países, impide la extradición pasiva de sus propios nacionales, en tanto y en cuanto ellos se encuentren dentro del territorio del cual ostentan esa calidad, cuestión a debatir seriamente, ya que este límite crearía una barrera por demás infranqueable, que impediría casi totalmente la aplicación de norma penal alguna, ya que dentro de la red es muy fácil cometer cualquier clase de delitos, sin abandonar el propio territorio, los cuales quedarían impunes en casi todos los casos, toda vez que si el país de origen no autoriza la extradición de sus nacionales, cualquier ordenamiento resultaría ineficaz, para aplicar sus procedimientos penales en ausencia del sujeto activo, al cual resulta imposible hacer comparecer a juicio.

En este punto, se cree que al menos para los delitos cometidos a través de la red y en virtud de la defensa de intereses comunes, debieran los Estados flexibilizar la postura, toda vez que son los mismos Estados, quienes pueden ser víctimas de las acciones ilegítimas por la red.

C) Análisis del Código Penal guatemalteco, Decreto Número 17-73

A pesar de que el Código Penal guatemalteco, data de los años 70, cuenta con normas que tienen aplicabilidad actualmente.

El Artículo 1 fundamentalmente es el que garantiza el principio de legalidad y manifiesta: "Nadie podrá ser penado por hechos que no estén expresamente calificados, como delitos o faltas, por ley anterior a su perpetración; ni se impondrán otras penas que no sean previamente establecidas en la ley".

Este principio rige para cualquier proceso y es reconocido universalmente en casi todas las legislaciones del mundo en materia penal.

También dentro de la normativa, prevalece principios que rige en el derecho internacional, especialmente cuando se trata de la territorialidad de la ley penal, al respecto, el Artículo 4 del Código Penal manifiesta: "Salvo lo establecido en tratados internacionales, este código se aplicará a toda persona, que cometa delito o falta en el territorio de la República o en lugares o vehículos sometidos a su jurisdicción".

Como se observa este principio se circunscribe al territorio taxativamente hablando del país, sin embargo, la siguiente normativa, se refiere a la extraterritorialidad y manifiesta el Artículo 5 que este Código también se aplicará:

"1o. Por delito cometido en el extranjero por funcionario al servicio de la República, cuando no hubiere sido juzgado en el país en el que se perpetró el hecho.

2o. Por delito cometido en nave, aeronave o cualquier otro medio de transporte guatemalteco, cuando no hubiere sido juzgado en el país en el que se cometió el delito.

3o. Por delito cometido por guatemalteco, en el extranjero, cuando se hubiere denegado su extradición.

4o. Por delito cometido en el extranjero contra guatemalteco, cuando no hubiere sido juzgado en el país de su perpetración, siempre que hubiere acusación de parte o del Ministerio Público y el imputado se hallare en Guatemala.

5o. Por delito que, por tratado o convención, deba sancionarse en Guatemala, aun cuando no hubiere sido cometido en su territorio.

6o. Por delito cometido en el extranjero contra la seguridad del Estado, el orden constitucional, la integridad de su territorio, así como falsificación de la firma del Presidente de la República, falsificación de moneda o de billetes de banco de curso legal, bonos y demás títulos y documentos de crédito".

En cuanto al análisis de esta norma no cabe duda que tiene limitaciones, especialmente si se refiere a los delitos informáticos, por cuanto la competencia para conocerlos, debe circunscribirse a estas reglas, y dentro de las mismas, no se establece nada al respecto, en el supuesto de que el delito se cometa en el territorio nacional, pero tiene efectos negativos o violatorio a derechos en otro Estado, que sucede al respecto o bien al contrario, cuando en otro Estado se comete el delito pero los efectos o resultados negativos, figuran en el territorio nacional y claro está, afectando a un nacional.

Al respecto de lo anterior, a pesar de que no es una respuesta adecuada técnicamente hablando, se encuentra la figura de la extradición, que como se señaló anteriormente, constituye una salida en caso de inexistencia de normas, que se refieran en forma directa acerca de la jurisdicción y competencia, en el caso de los delitos informáticos.

En el tema de la extradición, el Artículo 8 del Código Penal dice: "La extradición sólo podrá intentarse u otorgarse por delitos comunes. Cuando se trate de extradición comprendida en tratados internacionales, sólo podrá otorgarse si existe reciprocidad. En ningún caso, podrá intentarse ni otorgarse la extradición por delitos políticos, ni por delitos comunes conexos con aquéllos".

De acuerdo a lo anterior, se debe considerar lo siguiente:

a) Es evidente de que en el tema de la competencia, como la jurisdicción en materia de delitos informáticos y en cualquier otro delito, la tendencia del Código Penal guatemalteco, como la de muchos otros, es que se trata de delitos territoriales.

b) Lo anterior quiere decir, no se extienden más allá de sus fronteras y por ende, el Estado guatemalteco, no puede en principio perseguir penalmente a un ciudadano salvadoreño, o de cualquier otro país.

A pesar de que se reconoce, la existencia de tratados de extradición y de colaboración internacional, es claro que la potestad del Estado se limita a su territorio, tal como lo preceptúan las normas anteriores.

4.2 Competencia territorial y extraterritorial

Antes de describir algunas reglas de competencia respecto a los delitos informáticos, es importante señalar que podría ser un tema que interese al derecho penal internacional, es decir, mediante estas normas debieran resolverse 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.

Como por ejemplo, en un país cualquiera que modifica su Código Penal e incluye en éste, como delito al acceso no autorizado a sistemas de información. Luego, un banco sufre un acceso no autorizado, tendiente a obtener una transferencia indebida, se descubre quien accede, pero resulta que el violador del sistema, es de otra nacionalidad y que vive en Estados Unidos y que penetró en el sistema, a través de un servidor que se encuentra en Honduras.

Entonces, la pregunta es: ¿Podría el Estado en cuestión arrogarse la potestad de persecución del delito?

Este es un claro ejemplo, de lo que sucede generalmente en los delitos informáticos, y precisamente en normativas que no establecen claramente la jurisdicción y competencia para conocer de los mismos. En el caso de la Convención Contra el Ciber Crimen ya se regula, además se contempla, en la Ley de Delitos Informáticos que se encuentra en iniciativa y que se analizó arriba. Sin embargo, esta

problemática ha sido cuestionada por algunos tratadistas y éstos 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, como una regla que debe observarse.

Sin embargo en base a lo anterior, se podrían observar las siguientes reglas a seguir:

a) Por el lugar donde se cometió el hecho delictuoso o se realizó el último acto en caso de tentativa, o cesó la continuidad o la permanencia del delito.

b) Por el lugar donde se produjeron los efectos del delito.

c) Por el lugar donde se descubrieron las pruebas materiales del delito.

d) Por el lugar donde fue detenido el imputado.

e) Por el lugar donde se domicilia el imputado.

4.3 Presentación de los resultados del trabajo de campo

El trabajo de campo consistió en la realización de entrevistas respecto del tema, a abogados litigantes en el ramo penal, del Ministerio Público y la Defensa Pública Penal, por lo que se presentan los resultados del mismo en anexos.

De los resultados del trabajo de campo, se concluye que la totalidad de los entrevistados opinaron que los avances tecnológicos a través del Internet resultan de beneficio para la sociedad, sin embargo, también creen que estos avances pueden ocasionar un perjuicio respecto de las conductas indebidas, que con ellos pueden realizarse. Además estos profesionales manifestaron, que resulta complejo el regular

los delitos informáticos, y más complejo aún sancionarlos, ya que el Código Penal no se encuentra acorde con estas innovaciones del Internet.

4.4 Aspectos que se deben considerar para la solución de la problemática planteada

Objeto de la ley, es la protección integral de los sistemas que utilicen tecnologías de información, así como la prevención y sanción de los delitos cometidos contra tales sistemas o cualesquiera de sus componentes, o de los cometidos mediante el uso de dichas tecnologías, en los términos previstos en esta ley.

Según la propuesta de ley los conceptos mínimos deben ser:

a) Tecnología de información: Rama de la tecnología que se dedica al estudio, aplicación y procesamiento de datos, lo cual involucra la obtención, creación, almacenamiento, administración, modificación, manejo, movimiento, control, visualización, transmisión o recepción de información en forma automática, así como el desarrollo y uso del "hardware", "firmware", "software", cualesquiera de sus componentes y todos los procedimientos asociados con el procesamiento de datos.

b) Sistema: Cualquier arreglo organizado de recursos y procedimientos diseñados para el uso de tecnologías de información, unidos y regulados por interacción o interdependencia, para cumplir una serie de funciones específicas, así como la combinación de dos o más componentes interrelacionados, organizados en un paquete funcional, de manera que estén en capacidad de realizar una función operacional o satisfacer un requerimiento, dentro de unas especificaciones previstas.

c) Data (datos): Hechos, conceptos, instrucciones o caracteres representados de una manera apropiada para que sean comunicados, transmitidos o procesados por

seres humanos o por medios automáticos, y a los cuales se les asigna o se les puede asignar un significado.

d) Documento: Registro incorporado en un sistema en forma de escrito, video, audio o cualquier otro medio, que contiene data o información acerca de un hecho o acto capaces de causar efectos jurídicos.

e) Computador: Dispositivo o unidad funcional que acepta data, la procesa de acuerdo con un programa guardado y genera resultados, incluidas operaciones aritméticas o lógicas.

f) Hardware: Equipos o dispositivos físicos considerados en forma independiente de su capacidad o función, que conforman un computador o sus componentes periféricos, de manera que pueden incluir herramientas, implementos, instrumentos, conexiones, ensamblajes, componentes y partes.

g) Firmware: Programa o segmento de programa incorporado de manera permanente en algún componente de hardware.

h) Software: Información organizada en forma de programas de computación, procedimientos y documentación asociados, concebidos para realizar la operación de un sistema, de manera que pueda proveer de instrucciones a los computadores, así como de data expresada en cualquier forma, con el objeto de que los computadores realicen funciones específicas.

i) Programa: Plan, rutina o secuencia de instrucciones utilizados para realizar un trabajo en particular o resolver un problema dado, a través de un computador.

j) Procesamiento de datos o de información: Realización sistemática de operaciones sobre data o sobre información, tales como manejo, fusión, organización o cómputo.

k) Seguridad: Condición que resulta del establecimiento y mantenimiento de medidas de protección, que garanticen un estado de inviolabilidad de influencias o de actos hostiles específicos, que puedan propiciar el acceso a la data de personas no autorizadas, o que afecten, la operatividad de las funciones de un sistema de computación.

l) Virus: Programa o segmento de programa indeseado, que se desarrolla incontroladamente y que genera efectos destructivos o perturbadores, en un programa o componente del sistema.

m) Tarjeta inteligente: Rótulo, cédula o carné que se utiliza como instrumento de identificación; de acceso a un sistema; de pago o de crédito, y que contiene data, información o ambas, de uso restringido sobre el usuario autorizado para portarla.

n) Contraseña (password): Secuencia alfabética, numérica o combinación de ambas, protegida por reglas de confidencialidad, utilizada para verificar la autenticidad de la autorización, expedida a un usuario para acceder a la data o a la información contenidas en un sistema.

ñ) Mensaje de datos: Cualquier pensamiento, idea, imagen, audio, data o información, expresados en un lenguaje conocido que puede ser explícito o secreto (encriptado), preparados dentro de un formato adecuado para ser transmitido por un sistema de comunicaciones.

o) Extraterritorialidad: Cuando alguno de los delitos previstos en la ley se cometa fuera del territorio de la República, el sujeto activo quedará sometido a sus disposiciones, si dentro del territorio de la República se hubieren producido efectos del hecho punible, y el responsable no ha sido juzgado por el mismo hecho o ha evadido el juzgamiento o la condena, por tribunales extranjeros.

p) Sanciones: Las sanciones por los delitos previstos en esta ley, serán principales y accesorias. Las sanciones principales concurrirán con las penas accesorias y ambas podrán también concurrir entre sí, de acuerdo con las circunstancias particulares del delito del cual se trate, en los términos indicados en la presente ley.

q) Responsabilidad de las personas jurídicas: Cuando los delitos previstos en esta ley fuesen cometidos por los gerentes, administradores, directores o dependientes de una persona jurídica, actuando en su nombre o representación, éstos responderán de acuerdo con su participación culpable. La persona jurídica será sancionada en los términos previstos en esta ley, en los casos en que el hecho punible haya sido cometido por decisión de sus órganos.

1) En el caso de los delitos contra los sistemas que utilizan tecnologías de información:

"a) Acceso indebido: Toda persona que sin la debida autorización o excediendo la que hubiere obtenido, acceda, intercepte, interfiera o use un sistema que utilice tecnologías de información, será penado con prisión y multa.

b) Sabotaje o daño a sistemas: Todo aquel que con intención destruya, dañe, modifique o realice cualquier acto que altere el funcionamiento o inutilice un sistema que utilice tecnologías de información o cualquiera de los componentes que lo conforman, será penado con prisión y multa. Incurrirá en la misma pena quien destruya, dañe, modifique o inutilice la data o la información contenida en cualquier sistema que utilice tecnologías de información o en cualquiera de sus componentes. La pena será de prisión y multa, si los efectos indicados en el presente artículo se realizaren mediante la creación, introducción o transmisión, por cualquier medio, de un virus o programa análogo.

c) Favorecimiento culposo del sabotaje o daño: Si el delito previsto en el artículo anterior, se cometiere por imprudencia, negligencia, impericia o inobservancia de las normas establecidas, se aplicará la pena correspondiente según el caso, con una reducción entre la mitad y dos tercios.

d) Acceso indebido o sabotaje a sistemas protegidos: Las penas previstas en los artículos anteriores, se deberán aumentar entre una tercera parte y la mitad, cuando los hechos allí previstos o sus efectos, recaigan sobre cualesquiera de los componentes de un sistema que utilice tecnologías de información protegido por medidas de seguridad, que esté destinado a funciones públicas o que contenga información personal o patrimonial de personas naturales o jurídicas.

e) Posesión de equipos o prestación de servicios de sabotaje: Quien importe, fabrique, distribuya, venda o utilice equipos, dispositivos o programas; con el propósito de destinarlos a vulnerar o eliminar la seguridad de cualquier sistema que utilice tecnologías de información; o el que ofrezca o preste servicios destinados a cumplir los mismos fines, será penado con prisión y multa.

f) Espionaje informático: Toda persona que indebidamente obtenga, revele o difunda la data o información contenidas en un sistema que utilice tecnologías de información o en cualquiera de sus componentes, será penada con prisión. La pena deberá ser aumentada de un tercio a la mitad, si el delito previsto en el presente artículo, se cometiere con el fin de obtener algún tipo de beneficio para sí o para otro. El aumento deberá ser la mitad a dos tercios, si se pusiere en peligro la seguridad del Estado, la confiabilidad de la operación de las instituciones afectadas o resultare algún daño para las personas naturales o jurídicas, como consecuencia de la revelación de las informaciones de carácter reservado.

g) Falsificación de documentos: Quien a través de cualquier medio, cree, modifique o elimine un documento que se encuentre incorporado a un sistema que utilice tecnologías de información; o cree, modifique o elimine datos del mismo; o incorpore

a dicho sistema un documento inexistente, será penado con prisión y multa. Cuando el agente hubiere actuado con el fin de procurar para sí o para otro algún tipo de beneficio, la pena se aumentará entre un tercio y la mitad. El aumento deberá ser de la mitad a dos tercios, si del hecho resultare un perjuicio para otro".

2) De los delitos contra la propiedad:

"a) Hurto: Quien a través del uso de tecnologías de información, acceda, intercepte, interfiera, manipule o use de cualquier forma un sistema o medio de comunicación para apoderarse de bienes o valores tangibles o intangibles de carácter patrimonial sustrayéndolos a su tenedor, con el fin de procurarse un provecho económico para sí o para otro, será sancionado con prisión y multa.

b) Fraude: Todo aquel que, a través del uso indebido de tecnologías de información, valiéndose de cualquier manipulación en sistemas o cualquiera de sus componentes, o en la data o información en ellos contenida, consiga insertar instrucciones falsas o fraudulentas, que produzcan un resultado que permita obtener un provecho injusto en perjuicio ajeno, será penado con prisión y multa.

c) Obtención indebida de bienes o servicios: Quien sin autorización para portarlos, utilice una tarjeta inteligente ajena o instrumento destinado a los mismos fines, o el que utilice indebidamente tecnologías de información para requerir la obtención de cualquier efecto, bien o servicio; o para proveer su pago sin erogar o asumir el compromiso de pago de la contraprestación debida, será castigado con prisión y multa.

d) Manejo fraudulento de tarjetas inteligentes o instrumentos análogos: Toda persona que por cualquier medio, cree, capture, grabe, copie, altere, duplique o elimine la data o información contenidas en una tarjeta inteligente o en cualquier instrumento destinado a los mismos fines; o la persona que, mediante cualquier uso indebido de tecnologías de información, cree, capture, duplique o altere la data o información en

un sistema, con el objeto de incorporar usuarios, cuentas, registros o consumos inexistentes o modifique la cuantía de éstos, será penada con prisión y multa. En la misma pena deberá establecerse que incurrirá quien, sin haber tomado parte en los hechos anteriores, adquiera, comercialice, posea, distribuya, venda o realice cualquier tipo de intermediación de tarjetas inteligentes o instrumentos destinados al mismo fin, o de la data o información contenidas en ellos o en un sistema.

e) Apropiación de tarjetas inteligentes o instrumentos análogos: Quien se apropie de una tarjeta inteligente o instrumento destinado a los mismos fines, que se haya perdido, extraviado o que haya sido entregado por equivocación, con el fin de retenerlo, usarlo, venderlo o transferirlo a una persona distinta del usuario autorizado o entidad emisora, será penado con prisión y multa. La misma pena se impondrá a quien adquiera o reciba la tarjeta o instrumento a que se refiere el presente.

f) Provisión indebida de bienes o servicios: Todo aquel que, a sabiendas de que una tarjeta inteligente o instrumento destinado a los mismos fines, se encuentra vencido, revocado; se haya indebidamente obtenido, retenido, falsificado, alterado; provea a quien los presente de dinero, efectos, bienes o servicios, o cualquier otra cosa de valor económico será penado con prisión y multa.

g) Posesión de equipo para falsificaciones: Todo aquel que, sin estar debidamente autorizado para emitir, fabricar o distribuir tarjetas inteligentes o instrumentos análogos, reciba, adquiera, posea, transfiera, comercialice, distribuya, venda, controle o custodie cualquier equipo de fabricación de tarjetas inteligentes o de instrumentos destinados a los mismos fines, o cualquier equipo o componente que capture, grabe, copie o transmita la data o información de dichas tarjetas o instrumentos, será penado con prisión y multa".

3) Delitos contra la privacidad de las personas y de las comunicaciones:

"a) Violación de la privacidad de la data o información de carácter personal: Toda persona que intencionalmente se apodere, utilice, modifique o elimine por cualquier medio, sin el consentimiento de su dueño, la data o información personales de otro o sobre las cuales tenga interés legítimo, que estén incorporadas en un computador o sistema que utilice tecnologías de información, será penada con prisión y multa. La pena se deberá incrementar de un tercio a la mitad, si como consecuencia de los hechos anteriores resultare un perjuicio para el titular de la data o información o para un tercero.

b) Violación de la privacidad de las comunicaciones: Toda persona que mediante el uso de tecnologías de información, acceda, capture, intercepte, interfiera, reproduzca, modifique, desvíe o elimine cualquier mensaje de datos o señal de transmisión o comunicación ajena, será sancionada con prisión y multa.

c) Revelación indebida de data o información de carácter personal: Quien revele, difunda o ceda, en todo o en parte, los hechos descubiertos, las imágenes, el audio o, en general, la data o información obtenidas por alguno de los medios indicados en la ley que se propone sus bases, será sancionado con prisión y multa. Si la revelación, difusión o cesión se hubieren realizado con un fin de lucro, o si resultare algún perjuicio para otro, la pena se debería aumentar de un tercio a la mitad".

4) De los delitos contra niños, niñas o adolescentes:

"a) Difusión o exhibición de material pornográfico: Todo aquel que, por cualquier medio que involucre el uso de tecnologías de información, exhiba, difunda, transmita o venda material pornográfico o reservado a personas adultas, sin realizar previamente las debidas advertencias, para que el usuario restrinja el acceso a niños, niñas y adolescentes, será sancionado con prisión y multa.

b) Exhibición pornográfica de niños o adolescentes: Toda persona que por cualquier medio que involucre el uso de tecnologías de información, utilice a la persona o

imagen de un niño, niña o adolescente con fines exhibicionistas o pornográficos, será penada con prisión y multa".

5) De los delitos contra el orden económico:

"a) Apropiación de propiedad intelectual: Quien sin autorización de su propietario y con el fin de obtener algún provecho económico, reproduzca, modifique, copie, distribuya o divulgue un software u otra obra del intelecto, que haya obtenido mediante el acceso a cualquier sistema que utilice tecnologías de información, será sancionado con prisión y multa.

b) Oferta engañosa: Toda persona que ofrezca, comercialice o provea de bienes o servicios, mediante el uso de tecnologías de información, y haga alegaciones falsas o atribuya características inciertas a cualquier elemento de dicha oferta, de modo que pueda resultar algún perjuicio para los consumidores, será sancionada con prisión y multa y deberá establecerse que esto es sin perjuicio de la comisión de un delito más grave".

Deben establecerse agravantes: La pena correspondiente a los delitos previstos en la presente ley, se incrementarán entre un tercio y la mitad:

"a) Si para la realización del hecho, se hubiere hecho uso de alguna contraseña ajena indebidamente obtenida, quitada, retenida o que se hubiere perdido.

b) Si el hecho hubiere sido cometido mediante el abuso de la posición de acceso a data o información reservada, o al conocimiento privilegiado de contraseñas, en razón del ejercicio de un cargo o función.

c) Agravante especial: La sanción aplicable a las personas jurídicas por los delitos cometidos será únicamente de multa, pero por el doble del monto establecido para el referido delito".

Respecto a las penas accesorias:

Además de las penas principales previstas en los capítulos anteriores, se deberán imponer necesariamente sin perjuicio de las establecidas en el Código Penal, las penas accesorias siguientes:

"1. El decomiso de equipos, dispositivos, instrumentos, materiales, útiles, herramientas y cualquier otro objeto que hayan sido utilizados para la comisión de los delitos.

2. El trabajo comunitario.

3. La inhabilitación para el ejercicio de funciones o empleos públicos; para el ejercicio de la profesión, arte o industria; o para laborar en instituciones o empresas del ramo, por un período que puede ser hasta tres (3) años después de cumplida o conmutada la sanción principal, cuando el delito se haya cometido con abuso de la posición de acceso a data o información reservadas, o al conocimiento privilegiado de contraseñas, en razón del ejercicio de un cargo o función públicas, del ejercicio privado de una profesión u oficio, o del desempeño en una institución o empresa privada, respectivamente.

4. La suspensión del permiso, registro o autorización para operar o para el ejercicio de cargos directivos y de representación de personas jurídicas vinculadas con el uso de tecnologías de información, hasta un período que puede ser de tres (3) años, después de cumplida o conmutada la sanción principal, si para cometer el delito el agente se hubiere valido o hubiere hecho figurar a una persona jurídica.

5. Divulgación de la sentencia condenatoria: El Tribunal podrá además, disponer la publicación o difusión de la sentencia condenatoria, por el medio que considere más idóneo.

6. Indemnización civil: En los casos de condena por cualquiera de los delitos que deben establecerse en la ley, se impondrá en la sentencia una indemnización en favor de la víctima, por un monto equivalente al daño causado. Para la determinación del monto de la indemnización acordada, el juez requerirá del auxilio de expertos".

CONCLUSIONES

1. Existe una falta de cultura entre la población guatemalteca, en relación a los delitos informáticos. Esto puede provocar que la sociedad, se vea afectada con ilícitos que se cometen; y que el Estado se vea en la necesidad de combatir este tipo de delitos, por lo que el componente educacional, es un factor clave en la minimización de esta problemática.

2. El Código Penal del año 70 no es congruente, con lo que sucede en la realidad, respecto al aparecimiento de nuevos hechos o actos, que constituyen violación a derechos fundamentales de la personas, que por mandato constitucional tienen que ser sancionadas por el Estado, a través del ejercicio del poder punitivo que le legitima para imponer delitos, sanciones y medidas de seguridad.

3. Es innegable de que el Internet, a pesar de que ha sido de beneficio para la humanidad, también representa un peligro latente, sobre todo con las personas que posean un nivel más técnico y adecuado en su uso, ya que se presta para cometer ilícitos que pretendan fines económicos o lucrativos.

4. Evidentemente se generan conflictos de jurisdicción y competencia, y a pesar de que existen reglas para su aplicación, el Código Penal no es suficiente porque no se encuentra acorde a las innovaciones del Internet, regulando las conductas indebidas y prohibidas con su uso.

5. En el Código Penal guatemalteco, se encuentran reguladas algunas figuras delictivas que tienen relación con el uso de los computadores y el Internet, sin embargo tal como quedó establecido en el presente trabajo, su carácter generalizado no permite un encuadramiento eficaz, para una persecución y mucho menos para una sanción.


FACULTAD DE CIENCIAS JURIDICAS Y SOCIALES
UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
SECRETARIA
Guatemala, C. A.

RECOMENDACIONES

1. Es necesario que el Estado, a través de los entes encargados de creación de las leyes, como el Organismo Legislativo, conformen comisiones que estudien y analicen, la problemática que se suscita con el uso de la Internet, porque a la par de su utilización, también surgen criminales de nueva categoría en la comisión de hechos delictivos por este uso.

2. El Estado, en resguardo de la paz y la armonía en la sociedad, debe regular aquellas conductas que sean lesivas para que no afecten bienes jurídicos tutelados y legitimados, porque afectan derechos fundamentales de los ciudadanos.

3. El Estado de Guatemala, debe cumplir con los compromisos contraídos, como los distintos instrumentos jurídicos internacionales en materia de derechos humanos, porque dentro de ellos existe la preocupación mundial, para contrarrestar los hechos delictivos generados por el uso de la Internet, porque éstos, ponen en peligro los derechos fundamentales que asisten a las personas.

4. Los diputados al Congreso de la República, deben analizar la Ley de Delitos Informáticos que se encuentra en iniciativa, e incluir todo lo que haga falta respecto de la misma, para que entre en vigencia lo más pronto posible y de esa manera, contrarrestar la delincuencia que en la doctrina se ha denominado de cuello blanco.

5. Las instituciones como el Organismo Judicial, el Ministerio Público y el Instituto Público de la Defensa Penal, deben conformar comisiones, para promover iniciativas de ley que permitan adecuar las normas penales, a las realidades sentidas en cualquier materia, y principalmente en el caso del uso de la Internet y los abusos que se cometen en contra de los usuarios, porque dichos delitos

deben ser regulados, para que se puedan perseguir eficazmente y como consecuencia sancionarlos.

ANEXOS


FACULTAD DE CIENCIAS JURIDICAS Y SOCIALES
UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
SECRETARIA
Guatemala, C. A.

ANEXO 1

CUADRO No. 1

Pregunta: ¿Considera que los avances tecnológicos a través del Internet resultan de beneficio para la sociedad?

Respuesta	Cantidad
Si	10
No	00
Total	10

Fuente: Investigación de campo, marzo 2010

CUADRO No. 2

Pregunta: ¿Cree usted que a pesar de que resulta beneficioso para la sociedad los avances en la tecnología, también pueden ocasionar un perjuicio respecto de las conductas indebidas, que a través de los mismos pueden realizarse?

Respuesta	Cantidad
Si	10
No	00
Total	10

Fuente: Investigación de campo, marzo 2010

CUADRO No. 3

Pregunta: ¿Cree usted que resulta complejo el regular los delitos informáticos y más complejo aún, sancionarlos por el carácter internacional que los mismos tienen?

Respuesta	Cantidad
Si	10
No	00
Total	10

Fuente: Investigación de campo, marzo 2010

CUADRO No. 4

Pregunta: ¿Cree usted que el Código Penal se encuentra acorde a estas innovaciones, regulando conductas indebidas y prohibidas con el uso del Internet?

Respuesta	Cantidad
Si	05
No	05
Total	10

Fuente: Investigación de campo, marzo 2010

CUADRO No. 5

Pregunta: ¿Sabe usted si existe una ley en el Congreso de la República que abarque esta problemática?

Respuesta	Cantidad
Si	00
No	10
Total	10

Fuente: Investigación de campo, marzo 2010


FACULTAD DE CIENCIAS JURIDICAS Y SOCIALES
UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
SECRETARIA
Guatemala, C. A.

BIBLIOGRAFÍA

ANDRADE ABULARACH, Larry. **Derecho constitucional, derechos humanos**. Módulo 1. Escuela de Estudios Judiciales. Guatemala. 1999.

AYAU, Manuel. **Como mejorar el nivel de vida**. Volúmenes 1 y 2. Editorial Piedrasanta. Cordón y Gonzalo Asturias Montenegro. Guatemala. 1987.

BACIGALUPO, Enrique. **Lineamientos de la teoría del delito**. Editorial Hammurabi, S.R.L. 2ª. Edición. Buenos Aires, Argentina. 1989.

CARRIÒN, Hugo Daniel. **Presupuestos para la incriminación del Hawking**. Pág. 2.

CASTILLO GONZÀLEZ, Jorge Mario. **Comentarios, explicaciones e interpretación jurídica de la Constitución Política de Guatemala**. Editorial Impresiones Gráficas de Guatemala. Guatemala. 2002.

CASTILLO GONZÀLEZ, Jorge Mario. **Derecho administrativo**. Instituto Nacional de Administración Pública. 1990.

CEREZO MIR, José. **Curso de derecho penal español**. Parte General. Editorial Tecnos. 5ta. Edición. España.

COBO DEL ROSAL, M. y J. Boix Reig. **Garantías constitucionales del derecho sancionador**. Tomo I. Derecho penal y constitución.

COBO DEL ROSAL, M. y T. S. Vives Antón. **Introducción general sobre la reserva de ley orgánica y ley ordinaria en materia penal y administrativa en comentarios a la legislación penal**. Tomo III. Delitos e infracciones del estado civil. Madrid, España. 1984.

DE LA GARZA, Manuel. **Estudio sobre los delitos informáticos**. Pág. 98.

DE LEON CARPIO, Ramiro. **Catecismo constitucional**. Tipografía Nacional. Guatemala. 1995.

DE MATA VELA, José Francisco y Héctor Aníbal De León Velasco. **Derecho penal guatemalteco**. Editorial Llerena, S.A. Guatemala. 1998.

DE PAZ PÈREZ, Miguel. **Política administrativa del Estado de Guatemala**. Biblioteca de la Universidad de San Carlos de Guatemala. 1984.

Enciclopedia Encarta. 2002.

HANCE, Oliver. **Leyes y negocios en Internet**. Editorial Mc.Graw Hill. México. 1997.

JESCHECK, H. H. **Tratado de derecho penal**. Parte General. Tomo I. Traducido por Mir Puig y Muñoz Conde. Barcelona, España. 1981.

JIMÉNEZ DE ASÚA, L. **Tratado de derecho penal**. Tomo II. Filosofía y ley penal. Buenos Aires, Argentina. 1964.

PIEDRA SANTA, Rafael. **Introducción a los problemas económicos de Guatemala**. Volumen II. Editorial Universitaria. 1971.

Revista jurídica española la ley. **Delitos monetarios y reserva de ley orgánica**. Febrero de 1987.

RODRÍGUEZ DEVESA, J. M. **Derecho penal español**. Parte General. Madrid, España. 1985.

RODRÍGUEZ MOURULLO, G. **Derecho penal**. Parte General. Madrid, España. 1977.

RUIZ FRANCO, Arcadio. **Hambre y miseria en Guatemala**. Tipografía Nacional. 1950.

SANDOVAL RAMÌREZ, Luis. **La computación en el siglo veinte**. México. 1999.

SEIX, Francisco. **Derecho penal (principio de legalidad)**. Nueva Enciclopedia Jurídica Seix. Tomo XIV. Barcelona, España. 1978. Págs. 882 y ss.

SERRANO ALBERCA, J. M. **Comentarios a la constitución**. Madrid, España. 1980.

TÈLLEZ VALDEZ, Julio. **Los delitos informáticos**. Págs. 235, 246.

VIVES ANTÓN, T. S. **Introducción al estado de derecho y derecho penal**. Comentarios a la legislación penal. Tomo I. Derecho penal y constitución. Madrid, España. 1982.

www.ceue.com.htlm. Consejo de Europa. **Comité Europeo para los problemas de la delincuencia 25 de mayo 2001**, consulta 01- 03 – 2,010

www.goesjuridica.com.htlm, consulta 03-03-2,010

www.goesjuridica.com.htlm. Acalma Santos, Luis. **Problemas que se enfrenta por los conflictos de jurisdicción en el tema de los delitos informáticos**.3-3-2,010

www.monografías.com.htlm, consulta 02-03-2,010

www.onu.com.htlm. **Manual de Naciones Unidas para la Prevención y Control de Delitos Informáticos**, consulta 03-03-2,010

www.wikipedia.com.htlm. **Enciclopedia wikipedia,** consulta 02-03-2,010

www.wikipedia.com.htlm.**Historia del Internet y su evolución**, consulta 03-03-2,010

Legislación:

Constitución Política de la República de Guatemala. Asamblea Nacional Constituyente, 1986.

Código Civil. Decreto Ley número 106,1963 del Congreso de la República de Guatemala.

Código Penal. Decreto número 17-73 del Congreso de la República de Guatemala.

Código Procesal Penal. Decreto número 51-92 del Congreso de la República de Guatemala.

Convención Europea sobre el Ciber crimen. Budapest, Hungría. Noviembre 2001.

Iniciativa de Ley de Delitos Informáticos. Congreso de la República de Guatemala.

Ley del Organismo Ejecutivo. Decreto número 114-97 del Congreso de la República de Guatemala.

Ley del Organismo Judicial. Decreto número 2-89 del Congreso de la República de Guatemala.

Ley Orgánica del Congreso de la República. Decreto número 63-94 del Congreso de la República de Guatemala.