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

ANÁLISIS DE LA FALTA DE CAPACIDAD Y LEGISLACIÓN POR PARTE DEL ESTADO DE GUATEMALA EN RELACIÓN AL CIBERDELITO

TESIS

Presentada a la Honorable Junta Directiva

de la

Facultad de Ciencias Jurídicas y Sociales

de la

Universidad de San Carlos de Guatemala

Por

DUNIA LUCÍA RONCAL DUQUE

Previo a conferírsele el grado académico de

LICENCIADA EN CIENCIAS JURÍDICAS Y SOCIALES

y los títulos profesionales de

ABOGADA Y NOTARIA

Guatemala, septiembre 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. Modesto José Eduardo Salazar Diéguez
VOCAL V:	Br. Pablo José Calderón Gálvez
SECRETARIO:	Lic. Avidán Ortiz Orellana

TRIBUNAL QUE PRACTICÓ
EL EXAMEN TÉCNICO PROFECIONAL

Primera fase:

Presidenta:	Licda. Ileana Villatoro Fernández
Vocal:	Lic. Obdulio Rosales Dávila
Secretario:	Lic. Carlos Velásquez Polanco

Segunda fase:

Presidenta:	Licda. Mayra Veliz López
Vocal:	Lic. German Gómez Cachin
Secretaria:	Licda. Crista Ruiz de Juárez

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).

Licenciado Edgar Armindo Castillo Ayala
3 Avenida 13-62 zona 1
Teléfono: 2232-7936

Guatemala, 17 de mayo de 2011

Licenciado
Carlos Manuel Castro Monroy
Jefe de la Unidad de Asesoría de Tesis
Facultad de Ciencias Jurídicas y Sociales
Universidad de San Carlos de Guatemala

FACULTAD DE CIENCIAS JURIDICAS Y SOCIALES
RECIBIDO
17 MAYO 2011
UNIDAD DE ASESORIA DE TESIS
Hora:
Firma:

Licenciado Castro Monroy:

De conformidad con el nombramiento emitido por la Unidad de Asesoría de Tesis el día 23 de febrero del año 2011, procedí a asesorar el trabajo de Tesis de la Bachiller **DUNIA LUCÌA RONCAL DUQUE** el cual, luego de mi revisión, se titula:

"ANÁLISIS DE LA FALTA DE CAPACIDAD Y LEGISLACIÓN POR PARTE DEL ESTADO DE GUATEMALA EN RELACIÓN AL CIBERDELITO."

El trabajo de tesis de la Bachiller DUNIA LUCÍA RONCAL DUQUE, resalta la importancia de crear la legislación correspondiente por parte del Estado de Guatemala en pro de la protección que ha de brindar a los ciudadanos en el Ciberespacio.

Al hacer referencia al trabajo realizado por la Bachiller DUNIA LUCÍA RONCAL DUQUE, es necesario resaltar que el contenido científico y técnico de la tesis fue realizado con rigor, dedicación, estudio y análisis. En cuanto a la metodología, técnicas de investigación y redacción, cumplen las expectativas del objeto del trabajo, así también la investigación de campo, su análisis, conclusiones y recomendaciones.

De igual manera vale resaltar que fuera de las técnicas de investigación, con sumo cuidado se efectuaron las consultas bibliográficas, se realizaron los estudios doctrinarios, se aplicaron los métodos deductivo e inductivo y se utilizó un vocabulario jurídico adecuado.

Al emitir el **dictamen favorable**, me place manifestarle que el trabajo de mérito llena cada uno de los requisitos del Normativo contenido en el Artículo 32 para la Elaboración de Tesis de la Licenciatura en Ciencias Jurídicas y Sociales, por lo cual queda debidamente facultada para someterse al Examen General Público.

Sin otro particular me suscribo atentamente.

Lic. Edgar Armindo Castillo Ayala
Asesor de Tesis
Colegiado No. 6220

Edgar Armindo Castillo Ayala
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.

UNIDAD ASESORÌA DE TESIS DE LA FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES. Guatemala, veinticuatro de mayo de dos mil once.

Atentamente, pase al (a la) LICENCIADO (A): **MAYRA YANETH BARRAGÁN MALDONADO**, para que proceda a revisar el trabajo de tesis del (de la) estudiante: **DUNIA LUCÍA RONCAL DUQUE**, Intitulado: **"ANÁLISIS DE LA FALTA DE CAPACIDAD Y LEGISLACIÓN POR PARTE DEL ESTADO DE GUATEMALA EN RELACIÓN AL CIBERDELITO".**

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 las 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 estime pertinentes".

LIC. CARLOS MANUEL CASTRO MONROY
JEFE DE LA UNIDAD ASESORÌA DE TESIS

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FAC. DE C.C. J.J. Y S.S.
UNIDAD DE ASESORIA DE TESIS
GUATEMALA, C. A.

cc.Unidad de Tesis
CMCM/ brsp.

Guatemala, 3 de junio de 2011

LICENCIADO
CARLOS MANUEL CASTRO MONROY
JEFE DE LA UNIDAD DE ASESORÍA DE TESIS
FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES
UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
SU DESPACHO

Licenciado Castro Monroy:

De conformidad con la resolución en la cual se me designó REVISAR el trabajo de tesis de la bachiller **DUNIA LUCÍA RONCAL DUQUE**, carné número 200510714, titulado **"ANÁLISIS DE LA FALTA DE CAPACIDAD Y LEGISLACIÓN POR PARTE DEL ESTADO DE GUATEMALA EN RELACIÓN AL CIBERDELITO"** por este medio hago constar que se efectuaron las sesiones de trabajo para la revisión de mérito.

Al respecto considero que el trabajo presentado reúne los requisitos establecidos. He de manifestarle que la estudiante completó su investigación, la cual, tras correcciones que realicé, merece la siguiente opinión:

a) Contenido científico: la falta de capacidad y legislación por parte del Estado en cuanto al ciberdelito, deja en evidencia como esto, sólo crea una laguna legal que perjudica notablemente a los guatemaltecos y muy particularmente al hacer la comparación de derecho con otros países (derecho comparado) queda evidenciado la violación al derecho de seguridad y dignidad.

b) La utilización, dentro del trabajo de tesis, de técnicas de investigación bibliográficas de autores reconocidos en el ámbito jurídico, así como la investigación de campo, permitieron una práctica consulta de estudios doctrinarios a través de los métodos inductivo y deductivo; habiendo utilizado una redacción clara y técnica.

c) Las conclusiones son acertadas respecto al tema, con recomendaciones oportunas, las que estimo deben tomarse en consideración.

Confirmo que la bachiller atendió las sugerencias y observaciones señaladas, defendiendo con fundamento aquéllas que consideró necesarias y en general realizó el trabajo investigativo y analítico, redactando dicho trabajo con un lenguaje jurídico adecuado.

Por todo lo anteriormente señalado y en base al Artículo 32 del Normativo para la Elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Público, emito **DICTAMEN FAVORABLE** en el sentido que el trabajo de tesis desarrollado por la estudiante cumple con los requisitos establecidos.

Sin otro particular, me suscribo de usted atentamente,

Licda. Mayra Yaneth Barragán Maldonado
Revisor de tesis
Colegiado No.6 017

Licenciada
Mayra Yaneth Barragán Maldonado
Abogada y Notaria

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, dos de agosto del año dos mil once.

Con vista en los dictámenes que anteceden, se autoriza la Impresión del trabajo de Tesis del (de la) estudiante DUNIA LUCÍA RONCAL DUQUE, Titulado ANÁLISIS DE LA FALTA DE CAPACIDAD Y LEGISLACIÓN POR PARTE DEL ESTADO DE GUATEMALA EN RELACIÓN AL CIBERDELITO. Artículos 31, 33 y 34 del Normativo para la elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Público.-

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 ser siempre esa luz que ha guiado mi camino, por demostrarme día a día su infinita bondad al derramar tantas bendiciones en mi vida. Por permitirme llegar a este momento acompañada de los seres más maravillosos que con su amor ha creado.

A MIS PADRES: Por esta vida llena de experiencias mágicas, por ser parte de los buenos y los malos momentos, pues ha sido en estos donde me han dejado conocer que tan maravilloso y grandioso es el amor de un padre a sus hijos, por inculcar en mí los más puros sentimientos del bien. Dunia Marina Duque Morales, cómo agradecer todo el esfuerzo que has hecho en esta vida por mí, gracias por ser más que mi mamá por ser la amiga que siempre, siempre está ahí para mí, toda mi vida está marcada con tu ejemplo de bondad y sacrificio. Emilio Javier Roncal Martínez, gracias por ser ese ejemplo de generosidad y por la mejor enseñanza en mi vida "el amor al prójimo" gracias Inge por ser ese hombre que llena mi vida de emoción y le da ese tinte tan especial a mi día a día.

A MI HERMANA: Claudia María Roncal Duque, por ser la mejor compañera de batallas, gracias Claus por enseñarme que la mejor arma que tenemos para vencer, es el amor que hay entre nosotras, gracias porque me demuestras una y otra vez como tu amor y paciencia son claves para el funcionamiento de esto a lo que tú y yo muy humildemente hemos llamado "nuestra familia", gracias hermana por enseñarme las palabras claves de una profesional del derecho y gracias porque siempre has creído en mí.

A MIS ABUELAS: Ernestina Morales Barahona, mamá Tina, gracias por cada una de tus oraciones, sin duda alguna fueron esenciales para estar hoy acá, gracias por llenar mi vida de bendiciones. Alice de Roncal, ABY, por que fuiste el más claro ejemplo de superación en mi vida.

A MI FAMILIA: A mis mexicanísimos Roncalitos, a la familia Bracamonte, por ser parte de mi vida y por su apoyo incondicional.

A MIS AMIGOS: Tengo la bendición de decir gracias amigos por ser parte de mi vida, se que es imposible decir nombres, pero cómo dejar de mencionar a mis estimadísimas asuncionistas, a mis chicas del María y a ustedes compañeros universitarios, gracias por ser parte de mi historia San Carlista, gracias por ser parte de la mejor decisión de mi vida estudiar derecho, gracias por todos los momentos compartidos, y gracias por ser parte de mi gran evento.

EN ESPECIAL:

A: Licenciado Edgar Armindo Castillo Ayala por todas la enseñanzas compartidas y por hacer crecer en mi el amor por esta profesión. A la licenciada Mayra Yaneth Barragán Maldonado, por su orientación, apoyo, ejemplo y profesionalismo digno de admirar e imitar.

A: La tricentenaria, Universidad de San Carlos de Guatemala, y a la Facultad de Ciencias Jurídicas y Sociales, por el honor de ser parte de ellas y por inculcar en mí los valores necesarios para tan digna y admirable carrera.

ÍNDICE

Pág.

CAPÍTULO III

Pág.

CAPÍTULO IV

INTRODUCCIÓN

Guatemala, como un país en desarrollo ha enfrentado en la última década una serie de cambios estructurales en función de su economía, cultura, política, etc., y dentro de estos cambios estructurales se encuentran los avances tecnológicos, los cual viene a desencadenar una serie de efectos que para la sociedad es de suma importancia tratar, pues su no observancia violenta de manera evidente los derechos a la privacidad, a la seguridad y a la dignidad de las personas.

La definición del problema dentro de la presente investigación se estableció como la falta de interés del Estado de Guatemala, para resguardar la seguridad y dignidad de las personas en situaciones informáticas y la necesidad de crear programas, políticas y leyes aplicables a situaciones referentes al ciberdelito, mejorando las condiciones de las instituciones y de los sistemas de control.

La hipótesis planteada para este trabajo fue: La creación del ordenamiento jurídico relativo a la persecución de delitos cometidos en el sistema de red informática, coadyuvaría a garantizar el derecho de la seguridad y dignidad de la población guatemalteca.

El propósito del trabajo radica en determinar la necesidad de creación de programas, políticas y legislación para la persecución de acciones que atenten contra la seguridad y dignidad de las personas guatemaltecas, respetando el mandato constitucional del Estado de Guatemala.

La investigación se dividió en cuatro capítulos: El primer capítulo relativo a todas las generalidades sobre los sistemas de información por red, definiciones, algunas características y los servicios que se pueden prestar mediante estos; el segundo capítulo respecto al derecho humano a la seguridad y dignidad, definición, características y fundamento legal entre otros aspectos; el tercer capítulo se refiere a la legislación nacional e internacional respecto al ciberdelito y algunos delitos específicos en relación a la seguridad, dignidad y vida de las personas en los sistemas de información por red; y el capítulo cuarto contiene un análisis de la postura del Estado de Guatemala, ante el ciberdelito y como éste puede ser tratado por normas generales, dando a conocer el pensar y sentir de personas conocedoras del tema.

Para elaborar el informe final se utilizaron los métodos analítico para el estudio de la doctrina y la legislación, la síntesis para delimitar el área de estudio, el inductivo permitió elaborar paso a paso la investigación y el deductivo en la elaboración de resúmenes de contenido. La técnica utilizada en todo el análisis fue la bibliográfica.

Esperando que este trabajo contribuya de alguna manera para la discusión científica y legal de tan importante tema al Estado de Guatemala.

CAPÍTULO I

1. Aspectos generales sobre los sistemas de información en red

"Los Sistemas de Información y las Tecnologías de Información han cambiado la forma en que operan las organizaciones actuales. A través de su uso se logran importantes mejoras, pues automatizan los procesos operativos, suministran una plataforma de información necesaria para la toma de decisiones y, lo más importante, su implantación logra ventajas competitivas o reduce la ventaja de los rivales".[1]

"Las Tecnologías de la Información han sido conceptualizadas como la integración y convergencia de la computación, las telecomunicaciones y la técnica para el procesamiento de datos, donde sus principales componentes son: el factor humano, los contenidos de la información, el equipamiento, la infraestructura, el software y los mecanismos de intercambio de información, los elementos de política y regulaciones, además de los recursos financieros".[2]

Así entonces, podría indicar que los componentes anteriores conforman los protagonistas del desarrollo informático en una sociedad, tanto para su desarrollo como para su aplicación; además, se reconoce que las tecnologías de la información constituyen el núcleo central de una transformación multidimensional que experimenta la economía y la sociedad; de aquí lo importante que es el estudio y dominio de las influencias que tal

---

[1] http:/www.**monografia_sieteas de informacions**.com (Guatemala, 12 de diciembre de 2010).

[2]. http://www.**deltaasesores**.com (Guatemala, 12 de diciembre de 2010).

transformación impone al ser humano como ente social, ya que tiende a modificar no sólo sus hábitos y patrones de conducta, sino, incluso, su forma de pensar.

La información se ha colocado en buena medida como uno de los principales recursos que poseen las empresas actualmente. Los entes que se encargan de las tomas de decisiones han comenzado a comprender que la información no es sólo un subproducto de la conducción empresarial, sino que a la vez alimenta a los negocios y puede ser uno de los tantos factores críticos para la determinación del éxito o fracaso de estos.

"La fácil disponibilidad que poseen las computadoras y las tecnologías de información en general, han creado una revolución informática en la sociedad y de forma particular en los negocios",[3] pero también una serie de acciones que son ilegales y que son consideradas como delitos, propiamente denominados ciberdelitos.

"Un sistema de información es un conjunto de elementos que interactúan entre sí con el fin de apoyar las actividades de una empresa o negocio. En un sentido amplio, un sistema de información no necesariamente incluye equipo electrónico (hardware). Sin embargo en la práctica se utiliza como sinónimo de sistema de información computarizado".[4]

Un sistema de información realiza cuatro actividades básicas:

---

[3] Cohen Karen, Daniel. **Sistemas de información gerencial**. Pág. 32

[4] O´ Briend, James. **Bases de los sistemas de información**. Pág. 21

a. Entrada de información: proceso en el cual el sistema toma los datos que requiere para procesar la información, por medio de estaciones de trabajo, teclado, diskettes, cintas magnéticas, código de barras, etc.
b. Almacenamiento de información: es una de las actividades más importantes que tiene una computadora, ya que a través de ésta el sistema puede recordar la información guardada en la sesión o procesada anteriormente.
c. Procesamiento de la información: esta característica de los sistemas permite la transformación de los datos fuente en información que puede ser utilizada para la toma de decisiones, lo que hace posible, entre otras cosas, que un tomador de decisiones genere una proyección financiera a partir de los datos que contiene un estado de resultados o un balance general en un año base.
d. Salida de información: es la capacidad de un SI para sacar la información procesada o bien datos de entrada al exterior. Las unidades típicas de salida son las impresoras, graficadores, cintas magnéticas, diskettes, la voz, etc.

Los sistemas de información deben de cumplir con los siguientes objetivos:

a. Automatizar los procesos operativos.
b. Proporcionar información de apoyo a la toma de decisiones.
c. Lograr ventajas competitivas a través de su implantación y uso.

"Con frecuencia, los sistemas de información que logran la automatización de procesos operativos dentro de una organización son llamados Sistemas Transaccionales, ya que su función principal consiste en procesar transacciones tales como pagos, cobros, pólizas, planillas, entradas, salidas. Por otra parte, los sistemas de información que apoyan el

proceso de toma de decisiones son los Sistemas de Apoyo a la Toma de Decisiones (DSS, por sus siglas en inglés Decisión Supporting System). El tercer tipo de sistemas, de acuerdo con su uso u objetivos que cumplen, es de los Sistemas Estratégicos, los cuales se desarrollan en las organizaciones con el fin de lograr las ventajas competitivas, a través del uso de la Tecnología de Información".[5]

1.1. Importancia, funciones y misión de los sistemas de información

En cuanto a la importancia de los sistemas de información, debe establecerse que ésta radica en la utilidad y beneficios que ofrecen, pues facilitan a las empresas e instituciones que los utilizan, el manejo eficiente de los flujos de información necesarios para el desarrollo adecuado de las actividades de éstas; así pues, se entiende que el uso de los sistemas de información hoy en día es vital, siempre y cuando éste se haga de manera responsable.

"Por otro lado es importante tener una comprensión básica de los sistemas de información para entender cualquier otra área funcional en la empresa, por eso es importante también, tener una cultura informática en nuestras organizaciones que permitan y den las condiciones necesarias para que los sistemas de información logren sus objetivos".[6]

Dentro de las funciones y misión del sistema de información en red INFORNET está el proveer al comercio, de estudios completos y actualizados, de cómodo acceso y fácil interpretación, a bajo costo y alto valor, que aumente oportunidades y reduzca el riesgo

[5] Desantes Guanter, José María. **Hacia una historia del derecho a la información.** Pág. 22
[6] **Ibid.** Pág. 26

en las operaciones, principalmente cuando se trata de situaciones de crédito, pero no deja fuera del campo antecedentes sobre situaciones jurídicas pendientes y que pueden ser solicitadas por distintas empresas con intereses de contratar personal.

Asimismo, las funciones del sistema de información en red, a pesar de ser sus orígenes una empresa constituida en las Islas Vírgenes Británicas, hace accesible la mayor información posible que permite realizar análisis de créditos y otras negociaciones lícitas. El sistema de información es un intermediario en el traslado de la información y según su naturaleza no califica a las personas.

En Guatemala, las funciones de los sistemas de información por red, se encuentran activas desde hace 12 años, lo cual les otorga según su página de Internet: "La experiencia y la capacidad de elaborar los estudios más completos para personas individuales y empresas, ser el servicio más utilizado en Guatemala y con una importante y creciente presencia en el mercado centroamericano, siendo así que los servicios del sistema de información en red se ofrecen para Centroamérica por medio de colaboradores locales".[7]

Entre otras funciones específicas de las empresas de información por red en Guatemala, se pueden mencionar claramente las siguientes:

a. Información sobre clientes morosos en actividades crediticias.

[7] http://www.**infornet**.com (Guatemala ,17 de diciembre de 2010).

b. Situación de cualquier persona en relación a litigios o asuntos jurídicos en tribunales.

c. Además proporciona datos generales de las personas, tales como dirección, salario, estado civil, propiedades, etc.

Estas funciones han llegado a ocupar un lugar muy importante en la sociedad, e incluso se puede llegar a pensar que éstas se han vuelto esenciales para el desarrollo de toda empresa en el país, y de ahí el porque se han vuelto las funciones específicas, pues sin duda alguna son las que más ingresos les representan a dichas empresas de información por red.

1.2. Productos y servicios

"Los sistemas de información en red, tienen como servicios para satisfacer los diferentes objetivos e intereses de sus clientes, y a disposición de las personas varios productos, los cuales actualizan diariamente, siendo estos los siguientes:

a. Estudios Infornet: El producto más solicitado, tiene como finalidad proporcionar estudios con datos generales, referencias comerciales, judiciales, mercantiles y de prensa, que permiten al usuario realizar análisis y evaluaciones en el otorgamiento de créditos y otras actividades comerciales. Las referencias judiciales informan sobre demandas, querellas o denuncias presentadas, por lo general no reflejan el resultado de los juicios ni desistimientos o sobreseimientos de los mismos.

b. Estudios Prepagados Infornet: Similar al producto anterior, pero permite a los usuarios de pocos y esporádicos estudios utilizar los servicios sin realizar un contrato permanente. Tienen un tabla tarifaria para que los clientes puedan ver por la página el costo de lo que soliciten y cuánto les cuestan varios servicios, el cual es asignado en un precio de la moneda del dólar.

c. Estudios Batch: El cliente proporciona a Infornet en un archivo electrónico el listado de personas individuales o jurídicas, el listado es devuelto conteniendo los estudios requeridos en un archivo electrónico en el formato diseñado especialmente conforme los requerimientos establecidos por el cliente.

d. Preautorización de Créditos Infornet: Desarrollan preautorizaciones electrónicas en base a los requerimientos o perfiles de análisis de riesgos que al cliente le interesan. Este preautorizador puede ser visto vía Internet o en los archivos electrónicos que devuelve el servicio de estudios batch.

e. System to System: Conexión directa de servidores de clientes al servidor Infornet para aplicaciones ad-hoc (host to host).

f. Suministro de Información Crediticia a Infornet: El publicitar el comportamiento crediticio de sus clientes ofrece principalmente los siguientes beneficios:

- Se convierte en su mejor herramienta de cobro, reduciendo costos y esfuerzos;
- Mejora el comportamiento crediticio de los deudores;
- Hace más sanas las carteras de créditos; y

- Motiva a los demás intermediarios financieros a compartir sus referencias, ayudando a enriquecer la información, lo que permite tomar mejores decisiones y reducir los riesgos.

g. Actualizaciones Infornet: Las personas individuales o jurídicas, en cualquier momento pueden solicitar actualización o incorporación de sus datos o referencias, sin ningún costo y sin necesidad de contratar a un profesional, tampoco es necesario presentarse personalmente a las oficinas de cada país, la gestión puede hacerse por teléfono, fax o correo electrónico." [8]

Para la prestación de sus servicios estas empresas ofrecen e indican que el éxito en los negocios comienza con información confiable y que es necesario aprovechar la información integral y análisis avanzados para tomar mejores decisiones, desarrollar estrategias más rentables y mitigar el riesgo. Para ello en su información de la página de internet ponen a disposición una tabla tarifaria, basada en datos en dólares, que permite ver cuánto cuesta cada servicio y cuántos servicios por determinado valor de dinero; al confirmar que se solicita un servicio, ellos envían a un representante para firmar un contrato de confidencialidad y así ellos resguardan parte de su responsabilidad como empresas.

1.3. Fiabilidad

Cabe mencionar que la fiabilidad con la que cuentan estas empresas, se rige más que todo en que muchas empresas solicitan sus servicios, pero el principal punto de vista que atañe en relación a esta investigación es que mucha de la información establecida no

[8] http//www.**referencia**.infor.net (Guatemala, 20 de enero de 2010).

cuenta realmente con veracidad; y aun cuando las personas solventan sus situaciones la problemática sigue para ellos, por eso es necesario conocer sobre algunos antecedentes de la fiabilidad de estas empresas en Guatemala.

Sobre la fiabilidad de este tipo de empresas se puede mencionar la problemática del sistema de información en red, y los órganos del sistema de justicia; para el efecto se cita lo siguiente:

Con fecha veinte de mayo de dos mil tres, el periódico El Diario de Hoy del vecino país de El Salvador, en su pagina informativa indica que: "Guatemala cierra base de datos de Infornet, una resolución de la Procuraduría de los Derechos Humanos dio pie a la Fiscalía de Guatemala para poner fin a las operaciones de Infornet que comercializaba con la información de millones de salvadoreños." [9]

En resumen, la noticia indica que en Guatemala, Infornet no operará más y que la información privada y confidencial de millones de centroamericanos, entre ellos cuatro millones de salvadoreños, ya no sería vendida, señalando que la Fiscalía de Guatemala allanó el día diecinueve de mayo de dos mil tres la sede de la compañía guatemalteca, secuestrando todas las computadoras y servidores que le daban vida, en donde fiscales de El Salvador de la unidad anticorrupción querían verificar cuántos archivos de salvadoreños se encontraban ahí.

[9] http://www.**elsalvador.com/noticias**/2003/05/20/nacional/nacio20.html (Guatemala, 12 de julio de 2010).

Asimismo, dicha publicación menciona que el allanamiento a Infornet facilitará la investigación de hechos delictivos, y puesto que los datos podrían haberse utilizado para realizar otro tipo de actividades delictivas, como el secuestro o la extorsión; considerando esto último debido a que este sistema de información proporciona y sigue proporcionando a cualquier empresa o persona afiliada, todos los datos generales de las personas, lo cual es ilegal pues se viola el derecho a la intimidad de las personas, y bien puede considerarse como un ciberdelito.

Por otro lado, estos sistemas autorizados ofrecían y ofrecen hasta el momento, por medio de su empresa gemela (Transunion), la información de procesos mercantiles, civiles y penales no sólo de salvadoreños sino de muchos centroamericanos, sin dejar de mencionar la cantidad de guatemaltecos; lo que es extraño es que el acceso a esa información es confidencial, porque en materia civil y mercantil todo dato es de instancia privada; sólo tienen acceso las partes y ninguna otra persona ajena al caso; en materia penal hay casos de reserva.

También, en la misma noticia se estableció que Infornet había desaparecido del ciberespacio y que al intentar ingresar a su página en internet se corroboró que estaba fuera de servicio, pero eso fue en forma temporal ya que pocos días después y con la participación de la empresa gemela, pusieron a funcionar nuevamente la página.

También, el periódico Prensa Libre de Guatemala, el 20 de mayo de 2003, publicó que habían allanado la sede de Infornet, y que a partir del diecinueve de mayo el servicio de Infornet -venta de información personal y jurídica por la web- era irregular

La nota periodística señaló que: "En un operativo realizado por agentes del Ministerio Público y Policía Nacional Civil incautaron documentos y equipo de computación con el propósito de verificar si la compañía incurre en "delito informático", siendo así que los empleados de Infornet, una empresa que se dedica a recopilar información con fines lucrativos, recibieron una visita inesperada. Con orden de juez competente, la fiscal Blanca Lili Cojulún explicó al personal de la compañía que el "Ministerio Público efectuaba el operativo a raíz de una publicación de prensa, y que por ello se llevarían equipo y documentos que consideraran convenientes para sus pesquisas", esto lo índico en su momento Verónica Nájera, vocera de INFORNET en Guatemala. Se conoció que la Fiscalía, además del equipo decomisado, también quería las capturas de los trabajadores, pero el juez competente no accedió a este extremo".[10]

Dicha publicación además hace referencia a la violación del derecho a la privacidad, ya que de acuerdo con el Ministerio Público, una denuncia de la Procuraduría de los Derechos Humanos –PDH-, provocó el allanamiento y el decomiso de la información. El 14 de mayo, el Procurador de los Derechos Humanos, Sergio Morales, resolvió que: "Infornet violaba el derecho por injerencia arbitraria e ilegal, ya que la empresa no sólo da

[10] Méndez. Villaseñor, Claudia. **Allanan la sede de Infornet.** Pág 16.

conocer datos personales, sino que los publica, por lo que pidió a las autoridades respectivas que se investigará, y planteó la denuncia".[11]

Luego de todo lo expuesto, se puede decir que no existe total fiabilidad en relación a los sistemas de información que funcionan dentro de la red en Guatemala; por lo que es preocupante la problemática de falta de control por parte del Estado de Guatemala y de las instituciones respectivas para controlar este tipo de situaciones; puesto que no se tiene ningún grado de verificación de la información; además, este tipo de acciones son cometidas por empresas autorizadas legalmente, a quienes no les interesan todas aquellas personas individuales que se encuentran dentro del sistema de red.

1.4. Disponibilidad

Dentro de la disponibilidad de los sistemas de información por red, ofrecen el servicio de estudios de personas y sociedades por internet, el cual es de gran ayuda al empresario al otorgar créditos y contratar personal. El servicio va dirigido a toda empresa legalmente establecida en Guatemala, brindando diferentes opciones para trabajarlo; por ejemplo se estudia o analiza cualquier persona individual o jurídica antes de darles créditos o para contratar personal; o sea que, investigan su forma de vida, sus costumbres, qué propiedades o bienes posee, dónde y cuándo ha trabajado, si tiene o no deudas o créditos pendientes de pago o si tiene antecedentes penales o policiacos, entre otros datos.

[11] Morales, Sergio. **Informe circunstanciado.** Pág.123

1.5. Utilidad

Dentro de las utilidades para las empresas que ofrecen el sistema de información en red se encuentran las siguientes:

a. Historia de crédito: Se pueden tomar mejores decisiones crediticias cuando se comprende el nivel de riesgo que representa un cliente o prospecto; es mejor tomar decisiones a lo largo del ciclo de vida del cliente.

Las historias de crédito suministran información que se puede utilizar para adquirir más clientes, retener los más valiosos y administrar mejor el riesgo.

La información crediticia del sistema de información en red es suministrada y compartida por instituciones afiliadas. Estas entidades están comprometidas con mantener datos de alta calidad, entregando con regularidad información actualizada.

Las historias de crédito del sistema de información en red suministran información completa. Esto quiere decir que se registran y entregan datos positivos y negativos (La cantidad de datos positivos disponible puede variar según el mercado). Esto permite una visión más completa de la historia de crédito de un consumidor y mejora su capacidad para la toma de decisiones más objetivas.

Las historias de crédito pueden incluir los siguientes tipos de información:

- Información acerca del consumidor; como número de identificación, nombre y alguna información sociodemográfica adicional.

- Estado del cliente, una explicación breve acerca de los reclamos que haya presentado el titular de la información.
- Historia de cuentas, que incluyen el historial de pago del consumidor con los otorgantes de crédito.
- Registros públicos tales como demandas judiciales, quiebras y otra información disponible de origen público que pudiese afectar la capacidad de pago de sus clientes (Los tipos de información específica disponible pueden variar por mercado).
- Huella de consulta, nombre de las empresas afiliadas que han consultado la historia de crédito del consumidor.

Cuando se tiene acceso a mejor información acerca de los clientes y prospectos, se pueden tomar mejores decisiones; se pueden adquirir más clientes y retener a aquellos más valiosos, y al mismo tiempo pueden administrar mejor el riesgo.

La información es suministrada y compartida por los clientes del sistema de información en red. Cada entidad está comprometida a mantener la validez de la información suministrándola periódicamente y de manera actualizada.

La información es otorgada por las empresas crediticias, que a su vez subcontratan personas, usualmente personas de escasos recursos, para que éstas sean las encargadas de obtener dicha información; muy en concreto se puede ejemplificar cómo estos obtienen la información judicial que ofrecen de las personas individuales; estas

personas subcontratadas asisten diariamente a la torre de tribunales y de forma insospechada ingresan a los juzgados en donde se acercan a los libros de procesos ahí expuestos y toman datos de los mismos; siendo totalmente ilegal su forma de operar, pues dicha información sólo es pública para aquellas partes del proceso o las que de forma expresa demuestren tener interés en el mismo, pero he aquí una vez más la evidencia de cómo no existe protección a la información de los guatemaltecos.

b. Puntaje crediticio o credit scoring: El puntaje crediticio o credit scoring es un número que representa la calidad crediticia de un consumidor en un momento específico. Los puntajes o scores crediticios ayuda a evaluar el riesgo y tomar mejores decisiones, por parte de las empresas contratantes de los sistemas de información.

Este puntaje o score de crédito se genera mediante una fórmula matemática que utiliza datos de comportamiento crediticio históricos del consumidor, para calcular la posibilidad de ocurrencia de un evento en el futuro, aunque no indica que necesariamente dicho evento vaya a ocurrir.

El puntaje o score crediticio puede ayudar a comprender el estado financiero de los consumidores y a tomar decisiones más acertadas. También puede ayudar a reducir las ineficiencias asociadas a la subjetividad, errores manuales e información limitada. El puntaje o score crediticio también puede permitir reducir la exposición a determinados niveles de riesgo, cumplir con requisitos regulatorios e incrementar la rentabilidad de la cartera.

i. Score de buró: Permite a los otorgantes de crédito predecir la posibilidad de que un consumidor entre en mora de más de 90 días en una o más líneas de crédito durante los próximos 12 meses. Esto incluye tarjetas de crédito y préstamos para vivienda y automóviles, entre otros.

Este score predictivo fue desarrollado por un equipo global de analistas especializados de TransUnión; utilizando técnicas estadísticas y análisis avanzados. El modelo ha sido variado y ajustado mediante pruebas con instituciones financieras líderes en el mercado local. El sistema TransUnión Score Predictivo ayuda a automatizar los procesos y a facilitar decisiones más acertadas en un menor tiempo.

ii. Revisión de portafolio de cartera: La revisión del portafolio permite identificar de qué manera se distribuye el riesgo crediticio dentro de un portafolio de préstamos y cómo esa distribución puede cambiar con el tiempo. Esta revisión implica básicamente la evaluación del comportamiento crediticio de cada cliente en la cartera. Esto permite medir el riesgo que representa cada cliente del portafolio en ese preciso momento; y por lo tanto, la verdadera dinámica de riesgo subyacente de estos.

Esto puede ayudar a una mejor administración del riesgo crediticio, mejorar el retorno de la inversión y desarrollar un portafolio de productos para satisfacer mejor las necesidades de los clientes.

El portafolio de cartera es una herramienta valiosa para:

- Manejar las cuentas de clientes, ya que permite tomar decisiones oportunas y sólidas sobre límites de crédito, tasas de interés y términos de pagos.
- Administrar el portafolio de créditos y estar pendiente de cambios en el nivel de riesgo del mismo.
- Valorar el portafolio de cartera a través de una evaluación de su desempeño, logrando así tomar mejores decisiones de compra y venta de cartera, para reducir posibles pérdidas.

iii. Credit scoring a la medida: Los modelos de riesgo facilitan la toma de decisiones de aprobación o rechazo, haciéndolas sólidas, seguras y consistentes. Los modelos de scoring a la medida se utilizan para minimizar la exposición al riesgo mientras se aprovechan al máximo las oportunidades.

Los otorgantes de crédito también utilizan modelos para ayudar a incrementar los ingresos, reducir el incumplimiento y las pérdidas, identificar las cuentas más rentables y tomar decisiones más informadas a lo largo del ciclo de vida del cliente.

c. Gestión de cobranzas: Mientras más se sabe de los deudores, mayor probabilidad se tiene de recaudar la cartera de préstamos.

Una gestión de cobranzas rentable comienza con la evaluación de la capacidad de pago de un deudor; sin embargo, mayor información y conocimiento acerca de las probabilidades de recuperación pueden ayudar a tomar mejores decisiones. Aplicando técnicas avanzadas de análisis se puede ayudar a identificar cuáles cuentas tienen mayor probabilidad de pago y la estrategia más adecuada para gestionarlas.

Adicionalmente, los servicios de ubicación pueden ayudar a obtener direcciones y números de teléfono actualizados.

d. Servicios de mercadeo: Es aprovechar al máximo las oportunidades de mercadeo en el desafiante ambiente de los negocios de hoy con mejor información. Se puede incrementar el valor de los clientes que se tienen en la actualidad. Al combinar datos y análisis avanzados, se pueden encontrar y lograr oportunidades más rentables y alcanzar metas. Se pueden desarrollar estrategias que mejoran las relaciones y construyan fidelidad.

Cuando se sabe más acerca de los clientes se pueden desarrollar relaciones más profundas y construir fidelidad. Se pueden utilizar historias de crédito, puntajes o scores crediticios y demás servicios, para un mejor manejo del riesgo, venta cruzada de productos y definir estrategias de precios, entre otros. Se deben determinar los mercados correctos a los cuales entrar y a planear la estrategia apropiada.

e. Capacidad global: Ayuda a los negocios y consumidores en todo el mundo a lograr más cada día. Se combinan datos con técnicas de análisis y toma de decisiones, utilizando las mejores prácticas mundiales para crear soluciones poderosas que ayudan a los otorgantes de crédito a entender mejor a los consumidores en sus mercados locales.
Las formas como se puede ayudar a los negocios a lograr más cada día son:

i. Servicios de ventas y mercadeo: Los negocios se fortalecen cuando comprenden mejor los deseos y necesidades de los clientes. Se puede ayudar a desarrollar estrategias

e implantar programas que mejorarán las relaciones con ellos y construir fidelidad al tiempo que se incrementa la rentabilidad.

ii. Gestión de fraude e identidad: Cuando las empresas tienen un mejor sistema de identificación y manejo de las identidades se protegen más eficientemente a sí mismos y a sus clientes del fraude. Se pueden planear e implantar prácticas integrales de prevención del fraude y gestión de identidad. Esto ayuda a reducir las pérdidas debido al fraude, a fortalecer la confianza de los clientes en su marca y a reaccionar de manera más rápida y eficaz en el evento de un incumplimiento.

iii. Gestión de riesgo: Se combinan datos, técnicas de análisis y toma de decisiones con consultoría para ayudar a las empresas a tomar decisiones más sólidas. Esto les ayuda a aprovechar mejor las oportunidades y obtener mayor rentabilidad. Adicionalmente, productos para monitorear el comportamiento de las cuentas pueden identificar y anticipar cambios de manera proactiva para manejar fluctuaciones en la exposición al riesgo crediticio.

iv. Cumplimiento de las regulaciones: Es la información oportuna y completa, junto con tecnologías objetivas, no sesgadas, para ayudar a los clientes a mejorar sus programas de cumplimiento de las regulaciones.

v. Soluciones de información para el sector automotriz: La industria automotriz en los mercados locales en todo el mundo, puede aprovechar una amplia gama de datos de vehículos actualizada. Esto les ayuda a tomar mejores decisiones acerca del fraude, riesgo, valoración y eficiencia comercial.

1.6. Principales problemas en los sistemas de información

Actualmente, se está viviendo en una sociedad de información global emergente, con una economía global que depende cada vez más de la creación, la administración y la distribución de la información a través de redes globales como internet. Muchas empresas están en proceso de globalización; es decir, se están convirtiendo en empresas globales interconectadas en red.

Luego de todo lo expuesto y analizado en este capítulo, se pueden establecer los problemas que provocan los sistemas de información en red, tomando en cuenta la siguiente definición: "'Delito informático, crimen genérico o crimen electrónico, que agobia con operaciones ilícitas realizadas por medio de internet o que tienen como objetivo destruir y dañar ordenadores, medios electrónicos y redes de internet. Sin embargo, las categorías que definen un delito informático son aún mayores y complejas y pueden incluir delitos tradicionales como el fraude, el robo, chantaje, falsificación y la malversación de caudales públicos, en los cuales ordenadores y redes han sido utilizados. Con el desarrollo de la programación y de internet, los delitos informáticos se han vuelto más frecuentes y sofisticados".[12]

Esto implica entonces que el problema radica en todas aquellas actividades delictivas que se realizan por medio de dichas estructuras electrónicas; que van ligadas a infringir y dañar todo lo que encuentren en el ámbito informático: ingreso ilegal a sistemas, interceptado ilegal de redes, interferencias, daños en la información (borrado, dañado,

[12] http://www.estudding.org/**delito_inform** (Guatemala, 5 de enero de 2011).

alteración o supresión de datacredito), mal uso de artefactos, chantajes, fraude electrónico, ataques a sistemas, robo de bancos, ataques realizados por hackers, violación de los derechos de autor, pornografía infantil, pedofilia en internet, violación de información confidencial y muchos otros.


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

CAPÍTULO II

2. El derecho a la seguridad y dignidad

2.1. Derecho a la seguridad

La seguridad es un derecho fundamental y una de las condiciones del ejercicio de las libertades individuales y colectivas. El Estado tiene el deber de garantizar la seguridad en el territorio de la república, para defender las instituciones y los intereses nacionales, el respeto a las leyes, el mantenimiento de la paz y el orden público, la protección de las personas y los bienes.

El Diccionario de la Real Academia Española de la Lengua (DRAE), define el término de seguridad, entendiéndose por la seguridad de las personas, como sigue: "Término proveniente del latín seguritas. Cualidad de seguridad.// de seguridad. Loc. Adj. Que se aplica a un ramo de la administración pública cuyo fin es el de velar por la seguridad de los ciudadanos. Dirección general, agente de seguridad. Calidad de seguro, que se define como libre o ausente de todo peligro, daño o riesgo." [13]

Resulta importante señalar que la noción de seguridad tiene un aspecto subjetivo, que se refiere al sentimiento de un ciudadano de no tener peligro, y un elemento objetivo que se identifica con la ausencia real del mismo.

[13] http://www.rae.es/rae.html **definición de seguridad** (Guatemala, 15 de diciembre de 2010)

La seguridad de las personas se ha constituido en derecho constitucional consagrado en la mayoría de las Cartas Magnas de todos los países democráticos y en tal sentido los habitantes se encuentran protegidos en sus derechos por los Estados.

Según la Organización Regional de Naciones Unidas -CEPAL-, en el curso de preparación y evaluación de proyectos de seguridad ciudadana, llevado a cabo en 1997, la seguridad se definió: "Como la preocupación de los gobernantes por la calidad de vida y dignidad humana en términos de libertad, acceso al mercado y oportunidades sociales, para todos los individuos que comparten un entorno social delimitado por el territorio de un país".[14]

Dentro de un contexto sociológico, antropológico y jurídico se ha llegado a conocer que existen más de una docena de inseguridades que conforman la llamada seguridad ciudadana; como son: a la vida y el patrimonio; educación de calidad; salud; al trabajo; a la seguridad social (jubilación); alimentaria; al medio ambiente y ecología; jurídica; a la vivienda digna; a los derechos humanos, etc.

Dentro del derecho a la seguridad se deben entender dos conceptos importantes, como lo son el orden público que se define como la situación y estado de legalidad normal en que las autoridades ejercen sus atribuciones propias y los ciudadanos las respetan y obedecen sin protesta. Así también, lo que se define como seguridad pública que se define y hace referencia al mantenimiento de la paz y el orden público.

[14] http://www.pieb.org/seguridadciudadana/ **proyecto definición de seguridad** (Guatemala, 15 de diciembre de 2010)

En algunos países el término de seguridad pública sólo es considerada como un bien jurídico tutelado por el Estado dentro del ordenamiento jurídico.

2.1.1. Características

Dentro de las características de este derecho se encuentran las siguientes:

–Protege el derecho de las minorías.

–Aspira a la regulación de la convivencia.

–Propulsa el bienestar colectivo.

–El Estado es un ente regulador.

–La actividad del Estado está sometida al cumplimiento de la ley.

–Es una garantía del poder público ofrecido a la ciudadanía.

–Es un sistema de organización de la fuerza pública que cuida de manera eficaz impedir o reprimir las agresiones de que son víctimas las personas.

–La seguridad es hacer todo lo que la ley no prohíbe.

–Respeto al derecho de otros ciudadanos y los de la colectividad.

2.1.2. Elementos

Dentro de los elementos del derecho a la seguridad se puede mencionar primeramente al Estado de Guatemala. El Estado es una institución derivada de la convivencia humana en la forma más elevada, dentro de las condiciones de cada época y cada país. La libertad personal, el reconocimiento de la libertad de las naciones, la protección de las minorías y

el respeto a los derechos del hombre, deben seguir siendo la meta de toda política del Estado.

La esencia jurídica del Estado puede cifrarse en el hecho de constituir una organización que aspira a la regulación de la convivencia en un pueblo determinado; asentado sobre un cierto territorio, mediante la creación de una voluntad dominante sobre la totalidad de los ciudadanos.

Aunque el Estado pueda perseguir los fines individuales más diversos, es indudable que como comunidad teleológica tiene que propulsar el bienestar colectivo, en contraposición a los intereses de los individuos o de determinadas clases.

Para asegurar la vida individual del ciudadano sirven, en primer término, los derechos denominados fundamentales y de libertad. Moralidad, religión, cultura, ciencia, arte son también zonas libres. En ellas, la influencia del Estado puede ser a lo sumo indirecta. Otro tanto puede decirse de la libertad de movimiento y de la actividad económica; en ellas el Estado sólo influye de un modo regulador.

El siguiente elemento dentro del derecho a la seguridad, se encuentra el ciudadano que es el titular del derecho establecido por el ordenamiento jurídico constitucional por medio del Artículo 3, en el cual el Estado de Guatemala, está obligado a prestarle el beneficio de resguardar la seguridad e integridad del mismo. El espacio necesario para el ejercicio de la libertad en las relaciones interpersonales y sociales no se mantiene por sí solo. Entre más cercano es el contacto entre las personas, mucho más grande es el peligro de que las barreras de la libertad personal de cada uno sean rebasadas por los demás miembros

de la colectividad. Entre más sutil es el derecho de la libertad de una persona, más fácilmente puede este derecho ser violado por otros; es decir, entre menor capacidad de defensa de su derecho de libertad tenga una persona, mayor riesgo corre de que el mismo se vea invadido y violado por otros humanos.

Y el último elemento lo conforma la legislación conformada por la Constitución Política de la República de Guatemala, el Código Penal y los convenios y tratados internacionales firmados y ratificados por Guatemala.

2.1.3. Aspectos generales

El concepto tradicional de seguridad es el que lo asociaba con la represión del delito y el mantenimiento del orden; se trataba, pues, de un concepto de seguridad situada en el entorno del control y de la criminalidad y eminentemente reactiva.

La inseguridad, afecta a la esencia misma de la dignidad humana y a la vida en sociedad de suerte que; sin seguridad, no hay ejercicio posible e igualitario de los derechos de las personas. También es un problema complejo, que no se puede abordar simplemente, con el recurso tosco de penas más duras y más policías en la calle. Entonces, la pregunta que hace falta hacer, es la siguiente: cuáles son los elementos que hay que tener en cuenta en el abordaje a la inseguridad.

Se debe entender la superación de la vinculación cerrada entre seguridad y delincuencia, pero por una vía diferente: la del concepto subjetivo de inseguridad. La seguridad engloba, por lo tanto dos conceptos: por una parte, el objetivo, que estaría representado

por el incremento del delito y; por otro, el subjetivo que vendría determinado por la sensación de incertidumbre, de riesgo o de miedo que tiene el ciudadano por el desarrollo de lo que se denomina delincuencia ordinaria y los actos incívicos, diversos y no agrupables bajo una sola categoría pero que; no obstante, no entran dentro de la categoría de delitos. Delincuencia ordinaria y actos incívicos, se producen en el ámbito más próximo al ciudadano y; por lo tanto, afectan más directamente a su sensación térmica de seguridad.

La seguridad ciudadana entonces es el conjunto de medidas y previsiones que adopta el Estado a través de sus instituciones dentro del marco de la ley y los derechos humanos; para que la comunidad pueda desarrollar sus actividades libres de riesgo y amenazas.

También se debe entender que la seguridad es tarea de todos; pero para cumplir con estos cometidos es necesario que se acepten los cambios, que se estimulen las responsabilidades, romper marcos y buscar identificarse con el tema de la seguridad ciudadana. Todos tienen que ser parte de esta identificación con el problema para así poder comprometerse con la aceptación de los cambios.

Para el problema de seguridad, una de las soluciones viables es la prevención antes que la intervención desde la condición de ciudadanos y miembros de una comunidad o de un país. Se debe estar mucho más comprometidos con la sociedad, solidariamente participativos e incluso observar si alguien está incurriendo en alguna falta o en alguna negligencia que puede producir una desgracia, y así evitar la misma.

El tema de la seguridad pública es una de las preocupaciones permanentes de los ciudadanos, en casi todas las encuestas este tema ocupa uno de los primeros lugares; sin embargo, a esta preocupación no le sigue un nutrido debate, alentado por la sociedad misma, que lleve a mejores diagnósticos y al diseño de innovadoras alternativas para asegurar lo que también es un derecho humano.

2.1.4. Fundamentos legales

La Constitución Política de la República de Guatemala, como la ley de más alto nivel jerárquico en Guatemala y todas las demás leyes en observancia de la misma. "La Constitución es la ley básica que establece los principios y los derechos de todos los guatemaltecos; asimismo organiza jurídica y políticamente al Estado. Es la ley suprema, ya que todas las normas que ella contiene deben ser observadas y desarrolladas por las demás leyes y estas últimas nunca pueden ir en contra de la norma constitucional, pues de ser así se violentaría el principio de supremacía constitucional".[15]

En lo relativo al tema de la seguridad personal, este derecho está protegido por el Estado de Guatemala, así lo regula el Artículo 3º. de la Constitución Política de la República de Guatemala: "El Estado garantiza y protege la vida humana desde su concepción, así como la integridad y la seguridad de la persona".

Esto significa que el Estado de Guatemala debe garantizarle a todos, sin discriminación alguna, la seguridad, y esto se logra a través de las instituciones que el mismo Estado ha

[15] Asociación de Investigación y Estudios Sociales. **Derecho a la seguridad personal**. Pág. 12

creado para el efecto, así como con la creación de las nuevas instituciones necesarias para ese efecto.

Estas instituciones están obligadas a garantizar la seguridad, pues así lo manda la ley; y cuando la seguridad se vea en peligro o haya sido atacada, deben prestar ayuda, se les solicite o no. Todos los pueblos, y en el caso del pueblo guatemalteco deben reconocer los derechos humanos como base fundamental de toda sociedad para la consecución de la libertad y de la justicia mundial.

La Constitución Política de la República de Guatemala, dentro de la escala valorativa relacionada con la persona humana, ubica fundamentalmente la protección a la libertad y la seguridad, inmediatamente después del derecho a la vida. Como consecuencia de esta regulación constitucional era indudable que el derecho penal guatemalteco, hubiere incorporado dentro de su articulado aquellas figuras tradicionales que describen tipos delictivos contra la libertad y la seguridad, provenientes de códigos clásicos o positivistas; sin embargo, el desarrollo de la sociedad guatemalteca ha llevado a que el ordenamiento penal tenga que extenderse más allá de estas figuras y conceptualizar otros tipos penales.

El Código Penal regula, bajo el mismo título, los tipos penales que atentan contra la libertad y la seguridad como bienes jurídicos tutelados; pero también, contempla otros, bajo este mismo titulo, tales como: violación de la correspondencia y papeles privados, sustracción, desvío o supresión de correspondencia, turbación de actos de culto y

profanación de sepulturas. Todos estos tipos, tal como es nota característica del derecho penal conllevan, en el momento de realizarse, la imposición de una pena, la cual el mismo Código Penal gradúa en atención al delito, sus consecuencias y otras circunstancias objetivas y subjetivas que el juez debe de calificar. De tal manera que siendo la seguridad individual un derecho humano protegido y tutelado por el Estado, este mismo ha creado los mecanismos para que, como tal, sea garantizado y de esa manera crea un Código Penal que protege en contra de cualquier agresión de este derecho.

Por otro lado, la Declaración Universal de los Derechos Humanos, regula en el Artículo 3º que: "Todo individuo tiene derecho a la vida, a la libertad y a la seguridad de su persona".

La Declaración Americana de los Derechos y Deberes del Hombre, es un instrumento legal que tiene validez para todos los Estados del continente americano, como un código de conducta moral; su importancia radica en que es la primera Declaración que se aprueba a nivel supraestatal, para la vigencia de los derechos humanos en América, especialmente en lo que refieren los Artículos 1 y 5. El Artículo 1 establece que todo ser humano tiene derecho a la vida, a la libertad y a la seguridad de la persona; y el Artículo 5 establece que: "Toda persona tiene derecho a la protección de la ley contra los ataques abusivos a su honra, a su reputación y a su vida privada y familiar".

Así también, la Convención Americana sobre Derechos Humanos es la que da fuerza jurídica al articulado de la Declaración Americana de los Derechos y Deberes del Hombre. Esta Convención vino a reforzar el sistema interamericano de promoción y protección de

los derechos humanos. En el numeral 1 del Artículo 7, estipula que toda persona tiene derecho a la libertad y a la seguridad personal.

2.2. Derecho a la dignidad

Los valores se aprenden en el contexto de las primeras y más íntimas relaciones, con las familias, con la crianza religiosa y con las amistades más estrechas. Es en tales relaciones que se aprende la empatía y el querer, el honor, el respeto, la integridad y a ser justos. Mucho antes de empezar la carrera de abogado y notario, se aprenden estos valores fundamentales y se tienen muchas oportunidades para tomar decisiones críticas que involucran la verdad, la justicia y la dignidad humana.

La libertad es una condición imprescindible para la acción, que permite alcanzar a cada individuo los objetivos y fines morales que persiga, y que son la expresión de la dignidad humana, de su consideración como fin en sí, como algo valioso.

Los derechos del hombre son aquellos fundamentales de la persona humana, considerada tanto en su aspecto individual como comunitario, que corresponden a éste por razón de su propia naturaleza (esencia, a un mismo tiempo, corpórea, espiritual y social), y que deben ser reconocidos y respetados por todo poder y autoridad y toda norma jurídica positiva, cediendo no obstante, en su ejercicio ante las exigencias del bien común.

Los diversos conceptos que se han dado acerca de los derechos humanos, están ligados a las diferentes teorías que existen acerca de su fundamento. "Cabe, repetir entonces, en términos generales que, mientras para los iusnaturalistas los derechos humanos constituyen un orden suprapositivo, absoluto y anterior al derecho, para los positivistas los derechos humanos únicamente existen y son efectivos al ser plasmados en normas jurídicas, para los historicistas se trata de derechos relativos de acuerdo a la época que se trate y, para quienes los fundamentan en una concepción ética, los derechos humanos corresponden a derechos morales centrados en la idea de la dignidad humana".[16]

La dignidad de las personas debe de tomarse en su sentido amplio como aquél en el cual se deben respetar los principios y la ética de una persona, ya que la dignidad se encuentra afectada cuando personas particulares o el mismo Estado, no respetan la vida privada y que no es objeto de discusión de las personas. Cuando se refiere a la vida privada, son todas aquellas acciones y decisiones que sólo afectan e interesan a las personas en particular; su forma de vestir, su forma de comer, su cultura, etc., y que por supuesto son acciones que no van en contra de la ley.

Al referirse al derecho a la dignidad es importante tomar en cuenta que se refiere al valor inherente del ser humano en cuanto ser racional, dotado de libertad y poder creador, pues las personas pueden modelar y mejorar sus vidas mediante la toma de decisiones y el ejercicio de su libertad; por lo tanto, ésta se concibe en el marco de las relaciones de unos seres humanos con otros; es decir, dentro de la vida social. Interesa la libertad como

[16]Morales Trujillo, Hilda. **Manual de aplicación para la calificación de violaciones a los derechos humanos**. Pág. 30

posibilidad de alcanzar con base en decisiones libres, los propios objetivos vitales dentro del grupo social y sin chocar con la libertad de los demás.

2.2.1. Características

- La presión social en cuanto a la dignidad de la persona ejercida por los semejantes puede y de hecho llega a apoyar la conducta positiva o negativa y destructiva de las personas.
- La dignidad de las personas se fortalece por las costumbres del grupo u organización a la que pertenece.

–La dignidad se fortalece en las ideas por el bien y de la naturaleza emoción y espiritual del ser humano.

–La dignidad humana no se alcanza plenamente pero es de vital importancia en la continua búsqueda para aumentar al máximo el potencial humano.

–La base de la dignidad humana se encuentra fortalecida en la libertad de hacer.

–La dignidad humana es el respeto a la acción integral del ser humano.

2.2.2. Elementos

Respecto al derecho a la dignidad humana, cabe mencionar que el elemento subjetivo esencial es la acción de respeto a la vida privada y el honor de las personas, en el ámbito social y que va de acuerdo a su actuar respetando toda legislación.

Dentro de los elementos personales se encuentra la persona como titular del respeto al derecho a la dignidad; y el Estado de Guatemala, de garantizar por medio de las instituciones respectivas el respeto de la dignidad de las personas.

2.2.3. Aspectos generales

Es decir, los derechos humanos son propios de la naturaleza humana, o dicho de otro modo, son esenciales a su propia naturaleza. El ser humano nace con ellos, están en él, nadie se los otorga ni reconoce ni siquiera el Estado, porque derivan de la ley natural. Se debe entender definitivamente que no es el Estado ni la ciudad ni la familia los que han hecho al hombre. Esta es apenas una necesidad condicional, un medio para que aquél realice mejor su finalidad completa.

Por eso es mejor que, siendo los derechos atributos inseparables de la persona humana, deben ser respetados sin reparo ni distinción alguna, por cuanto sus derechos dimanan de su naturaleza. Ninguna razón de Estado o persona puede justificar la violación de los derechos primordiales del hombre.

La validez universal de los derechos humanos es una cuestión práctica referida a la ratificación por las naciones del mundo, de la Declaración Universal de 1948 y los pactos internacionales posteriores de las Naciones Unidas. La idea central que se puede encontrar en todos los momentos históricos, será el reclamo por la vigencia de la dignidad humana. En cada época esta dignidad se realiza de acuerdo con las condiciones económicas, sociales, culturales y políticas, y sólo en el mundo moderno a través de los derechos fundamentales.

El Artículo 1 de la Declaración Universal de los Derechos Humanos, regula que: "Todos los seres humanos nacen libres e iguales en dignidad y derechos y dotados como están de razón y conciencia, deben comportarse fraternalmente los unos con los otros".

Así también el Artículo 2, estipula: "Toda persona tiene los derechos y las libertades proclamadas en esta declaración, sin distinción alguna de raza, color, sexo, idioma, religión, opinión política o de cualquier otra índole, origen nacional o social, posición económica, nacimiento o cualquier otra condición. Además, no se hará distinción alguna fundada en la condición política, jurídica o internacional del país o territorio de cuya jurisdicción dependa una persona, tanto si se trata de un país independiente, como de un territorio bajo administración fiduciaria, no autónomo o sometido a cualquier otra limitación de soberanía".

La dignidad entonces se constituye en el fundamento de los derechos humanos, y en ese sentido se puede deducir que si no se hace el debido reconocimiento de la dignidad no se puede reclamar el reconocimiento ni la vigencia estos derechos, aunque ellos se hallen reconocidos por las instancias internacionales y nacionales.

"Así también el valor igualdad, tiene su antivalor en la discriminación, es el principio inspirador de todos los derechos económicos, sociales y culturales. Suele ser considerado como una "metanorma", o una norma que establece un criterio por el que todas las demás normas se relacionen con los sujetos del derecho. Sintéticamente podría formularse así: para toda persona, si reúne las condiciones de aplicabilidad de una norma, debe aplicarse

ésta siempre de idéntica manera. Salvo que circunstancias relevantes justifiquen un tratamiento normativo diferente, en beneficio del sujeto afectado por tales circunstancias. Por ejemplo, respecto al derecho al sufragio la diferencia de sexo es irrelevante actualmente, pero la diferencia de edad -caso de un niño sin uso de razón- es relevante para un tratamiento normativo no idéntico".[17]

La dignidad es un atributo de toda persona sea individual o colectiva, y la Constitución Política considera a la dignidad humana, como algo natural de todo hombre, y en virtud de ello es que se encarga de destacar que su finalidad es exaltar la dignidad de la persona, reconociéndola como algo propio y natural de ella -no otorgada por el Estado- y limitándose a garantizarla, estableciendo para ello su carácter de inviolable. Una condición previa para el reconocimiento de los derechos humanos es la dignidad.

2.2.4. Fundamentos legales

La Constitución Política de la Republica de Guatemala en el Artículo 4, sobre la libertad e igualdad, norma que: "En Guatemala todos los seres humanos son libres e iguales en dignidad y derechos. El hombre y la mujer, cualesquiera que sea su estado civil, tienen iguales oportunidades y responsabilidades. Ninguna persona puede ser sometida a servidumbre ni a otra condición que menoscabe su dignidad. Los seres humanos deben guardar conducta fraternal entre sí".

[17] Noguera Alcalá, Humberto. **Teoría y dogmática de los derechos fundamentales**. Pág. 21

"El derecho a la libertad se encuentra consagrado en la Declaración Universal de los Derechos Humanos y prácticamente atraviesa por sí misma o en interrelación con la dignidad, la igualdad, la integridad y la seguridad, todos los instrumentos internacionales de derechos humanos y está positivado en las Constituciones de los países occidentales, incluyendo la Constitución Política de la República de Guatemala, en cuanto a la forma de organización de los poderes del Estado y en el establecimiento de los derechos individuales, que descansan para su persistencia, en los derechos económicos, sociales y culturales".[18]

El Pacto Internacional de Derechos Civiles y Políticos, regula en sus Artículos 9, 10, 11, 12 y 13 el derecho de todo individuo a la libertad; las garantías que deben de gozar las personas que sean detenidas y las privadas de libertad; la imposibilidad de encarcelar a una persona que incumpla con obligaciones contractuales; el derecho de las personas de circular libremente en el territorio de un Estado en el que se encuentre legalmente y a escoger en él libremente su residencia.

Por su parte la Convención Americana sobre Derechos Humanos, se refiere al derecho a la libertad y por ende a la dignidad en su Artículo 7, en cuyo inciso 7 estipula que nadie será detenido por deudas, salvo el caso de incumplimiento de los deberes alimentarios. En el Artículo 8 regula las garantías judiciales para las personas detenidas y privadas de libertad. En el Artículo 9 se refiere al principio de legalidad y a la retroactividad de la ley. En el Artículo 12 regula el derecho a la libertad de conciencia y de religión; en el Artículo

[18] Morales Trujillo, Hilda. **Ob. Cit.** Pág. 38

13 se refiere a la libertad de pensamiento y de expresión; en el Artículo 15 a La libertad de reunión y en el 15 a la libertad de asociación.

Luego de todo lo expuesto y analizado en este capítulo se puede establecer que el derecho a la seguridad y dignidad son factores inherentes a todo ser humano, que emanan de la condición natural del hombre y es través de los distintos cuerpos normativos que el Estado los reconoce a cada persona, mas no los otorga.

En Guatemala, no se respeta el derecho a la seguridad y dignidad de los seres humanos; estos se ven violentados diariamente a través de la comisión de faltas y delitos por parte de las empresas de procesamientos de datos por red; entre otras acciones que también irrespetan estos derechos; y de esta forma se incumple con todo lo establecido por los diversos cuerpos normativos, ya señalados en esta investigación.

Corresponde al Estado de Guatemala como ente que ha de velar por el cumplimiento de los derecho humanos, hacer respetar el derecho a la seguridad y dignidad de las personas, pues el Estado a través de sus distintos organismos y en el cumplimiento de las funciones propias de cada uno de estos debe hacer respetar el ordenamiento jurídico; estando éste conformado por la Constitución Política de la República de Guatemala, los convenios y tratados internacionales, las normas ordinarias, los reglamentos y las normas individualizadas; y así cumplir con el fin de todo cuerpo normativo, siendo éste estipular y normar las condiciones necesarias para el adecuado desarrollo de la sociedad.


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

CAPÍTULO III

3. Legislación nacional e internacional referente a los ciberdelitos

3.1. Legislación nacional en relación a delitos contra la confidencialidad, la integridad y la disponibilidad de los sistemas y datos informáticos

En la legislación guatemalteca existen tres cuerpos legales que hoy en día, enmarcan situaciones en las que pueden verse violentados el derecho a la seguridad y la identidad a través de acciones contrarias al ordenamiento jurídico y que pueden realizarse por medio de los sistemas de información por red; siendo estos: la Constitución Política de la República de Guatemala, el Código Penal y la Ley de Acceso a la Información Pública.

La Constitución Política de la República de Guatemala, regula en el Artículo 35 sobre la libertad de emisión del pensamiento, el cual en forma literal estipula: "Es libre la emisión del pensamiento por cualesquiera medios de difusión, sin censura ni licencia previa. Este derecho constitucional no podrá ser restringido por ley o disposición gubernamental alguna". Pero lo fundamental es la parte última de este Artículo en que regula: "Quien en uso de esta libertad faltare al respeto a la vida privada o a la moral, será responsable conforme a la ley. Quienes se creyeren ofendidos tienen derecho a la publicación de sus defensas, aclaraciones y rectificaciones".

Asimismo, la Constitución Política de la República de Guatemala en el Artículo 24 regula que: "La correspondencia de toda persona, sus documentos y libros son inviolables... Se garantiza el secreto de la correspondencia y de las comunicaciones telefónicas,

radiofónicas, cablegráficas y otros productos de la tecnología moderna". O sea que este Artículo protege la privacidad de las personas.

El derecho de la seguridad como elemento inherente al ciudadano se ve protegido según el ordenamiento jurídico constitucional por medio del Artículo 3, que regula que el Estado de Guatemala, está obligado a resguardar la seguridad e integridad del mismo y dentro de esa función está el respeto a la privacidad; por lo que el Estado está obligado a verificar y velar por su cumplimiento.

El Artículo 2 de la Constitución Política de la República de Guatemala, norma que es deber del Estado garantizar a sus habitantes la vida, la libertad, la justicia, la seguridad, la paz y el desarrollo integral de la persona. De lo expuesto se debe de entender que cuando se refiere a la seguridad también se refiere a la seguridad jurídica, siendo necesario aclarar que es el Estado el que debe hacer respetar el ordenamiento jurídico y velar por el fiel cumplimiento del mismo y así otorgar dicha seguridad.

Otro fundamento constitucional es el Artículo 4, sobre la libertad e igualdad: "En Guatemala, todos los seres humanos son libres e iguales en dignidad y derechos... Ninguna persona puede ser sometida a servidumbre ni a otra condición que menoscabe su dignidad. Los seres humanos deben guardar conducta fraternal entre sí". Esto implica el respeto a la privacidad de las demás personas.

Por último, también se puede fundamentar el derecho a la privacidad por medio del Artículo 14, que trata sobre la presunción de inocencia y publicidad del proceso, estipulando que: "Toda persona es inocente, mientras no se haya declarado responsable judicialmente, en sentencia debidamente ejecutoriada". Esto quiere decir que mientras no exista una decisión definitiva judicial o recursos procesales en contra de la misma, nadie puede hacer una proyección de los datos o declarar la culpabilidad o inocencia del procesado.

Por otro lado el Código Penal guatemalteco, regula en su Artículo 274 incisos "D" y "F", la limitación sobre datos personales así:

"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 u otro registro informático con datos que puedan afectar la intimidad de las personas".

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

Lo anterior demuestra que la legislación en materia penal, encuadra una figura que puede permitir accionar en contra de empresas que manejan datos personales, mas no logra cubrir por completo el campo cibernético actual; por lo que se debe complementar con la Ley de Acceso a la Información Pública, creada por el Congreso de la República Guatemala , mediante el Decreto número 57-2008, y aun cuando su naturaleza es sobre

el acceso a la información pública, establece tres Artículos que limitan el uso de datos personales. Su parte considerativa regula que la Constitución Política de la República de Guatemala, dentro de sus fines considera la vida, la libertad y la seguridad de las personas; lo que puede ser tomado como parte del ordenamiento jurídico que fortalece el derecho a la privacidad.

La Ley de Acceso a la Información Pública establece los siguientes Artículos referentes a la privacidad, que desarrollan el respeto a la seguridad y dignidad de las personas individuales y de las personas jurídicas, por medio de sistemas de información por red.

"Artículo 15. Uso y difusión de la información. Los interesados tendrán responsabilidad, penal y civil por el uso, manejo o difusión de la información pública a la que tengan acceso, de conformidad con esta ley y demás leyes aplicables".

"Artículo 17. Consulta personal. Los sujetos deben tomar todas las medidas de seguridad, cuidado y conservación de los documentos, elementos o expedientes de cualquier naturaleza, propiedad del sujeto obligado que le fueren mostrados o puestos a disposición en consulta personal; así como hacer del conocimiento de la autoridad competente toda destrucción, menoscabo o uso indebido de los mismos, por cualquier persona".

"Artículo 64. Comercialización de datos personales. Quien comercialice o distribuya por cualquier medio, archivos de información de datos personales, datos sensibles o personales sensibles, protegidos por la presente ley sin contar con la autorización expresa

por escrito del titular de los mismos y que no provengan de registros públicos, será sancionado con prisión de cinco a ocho años y multa de cincuenta mil a cien mil quetzales y el comiso de los objetos instrumentos del delito. La sanción penal se aplicará sin perjuicio de las responsabilidades civiles correspondientes y los daños y perjuicios que se pudieran generar por la comercialización o distribución de datos personales, datos sensibles o personales sensibles".

Los anteriores Artículos regulan ya, además de lo que estipulan el Código Penal de Guatemala, figuras y sanciones; el problema radica en cómo se fiscalizará el uso de la información, y el vacío legal en que se incurrió al momento de no establecer específicamente que las empresas privadas y crediticias por medio de documentos hicieren renunciar a las personas de sus derechos de privacidad.

3.2. Legislación nacional en relación a delitos informáticos

La legislación guatemalteca se refiere a este tipo de delitos en el Capítulo VII del Título VI del Código Penal, Decreto número 17-73, del Congreso de la República de Guatemala; delitos contra el derecho de autor, la propiedad industrial y delitos informáticos.

Así también, dentro del mismo cuerpo legal se establece lo referente a la destrucción de registros informáticos, que regula en el literal A del Artículo 274: "Será sancionado con prisión de seis meses a cuatro años, y se aplicará multa de doscientos a dos mil quetzales, el que destruyere, borrare o de cualquier modo inutilizare registros informáticos". Debe así pues entenderse que cualquier persona que realice acciones que conlleven la destrucción, pérdida o inutilización de información que se encuentre

registrada en los medios electrónicos, está realizando una acción que puede encuadrar en este tipo legal.

Respecto a la alteración de programas el Artículo 274 B, regula que: "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." Este literal hace referencia más bien a los comandos o formatos que utilizan los programas electrónicos para llevar a cabo distintas operaciones informáticas, y no a la información en sí a la que se refiere el literal anterior.

Sobre la reproducción de instrucciones o programas de computación el Artículo 274 C regula que: "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." En este literal puede observarse una redacción ambigua, en cuanto al conocimiento de términos técnicos en materia de informática, pues realmente puede entrase en una discusión sobre lo que el legislador realmente quiso dar a entender en dicho literal, y lo que se entiende en su contexto, quedando así una normativa abierta al no establecer claramente cuál es la conducta delictiva que contempla. La acción por medio de la cual se copian las instrucciones o programas de computación es técnicamente conocida como hackear.

Sobre los registros prohibidos Artículo 274 D se norma que: "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." Es justo este tipo penal en donde se trata de encuadrar la actividad realizada

por las empresas procesadoras de información por red, pero así también una vez más se demuestra el poco alcance de la ley, pues no logra establecer claramente qué tipo de infracción afecta la intimidad de las personas, así como tampoco establece a qué tipo de personas se refiere, y a su vez delimita el grado de afectación de la información que se pueda publicar, pues ya se ha establecido que la información publicada en estos sitios virtuales violenta claramente no sólo la intimidad sino la seguridad y dignidad de las personas, así también deja afuera la forma de obtención de la información, que también hace incurrir a estas empresas en otras actividades delictivas que no se encuentran tipificadas.

Respecto a la manipulación de información el Artículo 274 E: "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". El ciberespacio permite realizar todo tipo de actividades ilícitas, las actividades relacionadas a la estafa en cuanto a venta de productos, suele ser la más común, pues muchos sitios de internet ofrecen productos o servicios que posteriormente son entregados al comprador sin llenar los requisitos o exigencias del mismo en cuanto a lo ofrecido; siendo estas negociaciones a distancia y bajo condiciones no expuestas, lo que hace imposible el reclamo por parte del comprador encuadrando la actividad en una venta fraudulenta. Este literal también hace referencia a la posible defraudación tributaria que se puede dar por medio del uso de sistemas o programas virtuales que alteren datos contables.

Sobre el uso de información, regula el Artículo 274 F que: "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." Este literal evidencia la realización de actividades que violentan el derecho a la intimidad, y la clara violación a la propiedad privada, pero cabe hace mencionar la falta de regularización sobre lo que en la red o el cieberespacio ha de entenderse como propiedad privada, pues existen distintos portales que ofrecen a los usuarios el servicio de correo electrónico o email dando la oportunidad a los usuarios de contar con cuentas electrónicas en las que pueden recibir y enviar todo tipo de información ya sea a otras cuentas electrónicas o de otros portales; pero al momento de que el usuario realiza el contrato virtual con el portal que ofrece este servicio, le otorga todos los permisos para que su cuenta electrónica sea escaneada y la información entonces obtenida por estos medios jamás es confidencial o completamente privada; pues a pesar de que otras personas no puedan tener acceso a dichas cuentas electrónicas sí permite que el proveedor del servicio esté en constante vigilancia de la información manejada por este medio; es entonces un correo electrónico propiedad privada, debe entenderse que no, pues dicho servicio tiene sus limitaciones, cosa que no sucede con la propiedad privada, pues su extensión es claramente limitada.

En lo que se refiere a los programas destructivos regula el cuerpo legal en el Artículo 274 G que: "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". Existen distintos programas o comandos que pueden destruir la

información almacenada en otros canales o sitios virtuales; muchas veces estos son vendidos o simplemente puestos en circulación a través de la red y el daño que causan puede llegar a ser irreparable y millonario; pues usualmente se utilizan para desactivar candados de seguridad que las empresas utilizan para mantener su información a salvo; así también son utilizados para infiltrarse y obtener información confidencial que las personas han puesto en sitios virtuales.

Estos Artículos vienen a fundamentar la clasificación mencionada sobre los hechos ilícitos en relación a delitos informáticos; y establecen y encuadran algunas figuras, pero deja muchas de esas acciones sin una verdadera sanción, tal como se observará en el siguiente punto.

3.3. Legislación en relación a delitos relativos al contenido

A nadie escapa la enorme influencia que ha alcanzado la informática en la vida diaria de las personas y organizaciones, y la importancia que tiene su progreso para el desarrollo de un país. Las transacciones comerciales, la comunicación, los procesos industriales, las investigaciones, la seguridad, la sanidad, etc., son todos aspectos que dependen cada día más de un adecuado desarrollo de la tecnología informática.

Junto al avance de la tecnología informática y su influencia en casi todas las áreas de la vida social; han surgido una serie de comportamientos ilícitos denominados, de manera genérica, delitos informáticos. La informática está hoy presente en casi todos los campos de la vida moderna. Con mayor o menor rapidez todas las ramas del saber humano se

rinden ante los progresos tecnológicos, y comienzan a utilizar los sistemas de información para ejecutar tareas que en otros tiempos realizaban manualmente.

El progreso cada día más importante y sostenido de los sistemas computarizados permite hoy procesar y poner a disposición de la sociedad una cantidad creciente de información de toda naturaleza, al alcance concreto de millones de interesados y de usuarios. Las más diversas esferas del conocimiento humano, en lo científico, en lo técnico, en lo profesional y en lo personal están siendo incorporadas a sistemas informáticos que, en la práctica cotidiana, de hecho sin limitaciones, entregan con facilidad a quien lo desee un conjunto de datos que hasta hace unos años sólo podían ubicarse luego de largas búsquedas y selecciones en que el hombre jugaba un papel determinante y las máquinas existentes tenían el rango de equipos auxiliares para imprimir los resultados. En la actualidad, en cambio, ese enorme caudal de conocimiento puede obtenerse; además, en segundos o minutos, transmitirse incluso documentalmente y llegar al receptor mediante sistemas sencillos de operar, confiables y capaces de responder casi toda la gama de interrogantes que se planteen a los archivos informáticos; además, las fuentes de información ofrecen información actualizada, minuto a minuto, los sistemas informáticos se han llegado a globalizar de tal manera que no existe actualmente tema que no pueda ser investigado a través de la red. Así también, la forma más común y eficiente de realizar todo tipo de comunicaciones, ya sean, familiares, sociales, laborales, académicas, etc., es la vía electrónica, asegurando una inmediata realimentación en esta comunicación.

"Es así entonces como de acuerdo con la definición elaborada por un grupo de expertos, invitados por la Organización de Cooperación y Desarrollo Económico (OCDE) a París en

mayo de 1983, el término delitos relacionados con las computadoras se define como cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesado automático de datos y/o transmisiones de datos. La amplitud de este concepto es ventajosa, puesto que permite el uso de las mismas hipótesis de trabajo para toda clase de estudios penales, criminólogos, económicos, preventivos o legales". [19]

Así también, dentro de las características de los delitos, según el mexicano Julio Tellez Valdez, los delitos informáticos 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) puede llegar a cometerlas.
b. Son acciones ocupacionales, en cuanto a que muchas veces se realizan cuando el sujeto desarrolla las actividades propias de sus labores diarias.
c. Son acciones de oportunidad, ya que se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico.
d. Provocan serias pérdidas económicas, ya que casi siempre producen beneficios económicos para aquellos quienes lo realizan, perjudicando así al agraviado.
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.

[19] http://arbitrajeglobal.com/**artículos delito_informatico**(Guatemala, 22 de enero de 2011)

g. Presentan grandes dificultades para su comprobación, esto por su mismo carácter técnico.
h. la tendencia de aumento cada vez es mayor, por lo que requieren una urgente regulación. Por el momento siguen siendo ilícitos impunes de manera manifiesta ante la ley". [20]

Luego de lo expuesto, se puede indicar que aun cuando no existe una legislación específica sobre los ciberdelitos o delitos informáticos; dichas acciones pueden existir y encuadran dentro de una norma jurídica guatemalteca; por ello para el análisis respectivo se cita una de las clasificaciones generales sobre delitos informáticos y si los mismos encuadran en alguna figura de la legislación guatemalteca, siendo ésta la siguiente:

a. Según la actividad informática

A. **Sabotaje informático**: El término sabotaje informático comprende todas aquellas conductas dirigidas a causar daños en el hardware o en el software de un sistema. Los métodos utilizados para causar destrozos en los sistemas informáticos son de índole muy variada y han ido evolucionando hacia técnicas cada vez más sofisticadas y de difícil detección. Básicamente, se pueden diferenciar dos grupos de casos: por un lado, las conductas dirigidas a causar destrozos físicos y, por el otro, los métodos dirigidos a causar daños lógicos.

[20] Tellez, Julio **Derecho informativo. Sistematización y consolidación del derecho, legislación y el manejo de la información en la era del conocimiento**. Pág. 63

a. **Conductas dirigidas a causar daños físicos**: El primer grupo comprende todo tipo de conductas destinadas a la destrucción física del hardware y el software de un sistema; por ejemplo: causar incendios o explosiones, introducir piezas de aluminio dentro de la computadora para producir cortocircuitos, derramar sustancias o agentes cáusticos en los equipos, etc. En general, estas conductas pueden ser analizadas, desde el punto de vista jurídico, en forma similar a los comportamientos análogos de destrucción física de otra clase de objetos previstos típicamente en el delito de daño.

b. **Conductas dirigidas a causar daños lógicos**: El segundo grupo, más específicamente relacionado con la técnica informática, se refiere a las conductas que causan destrozos lógicos, haciendo referencia a los daños en el sistema mismo o sea, todas aquellas conductas que producen, como resultado, la destrucción, ocultación, o alteración de datos contenidos en un sistema informático.

Este tipo de daño a un sistema se puede alcanzar de diversas formas. Desde la más simple que se puede imaginar, como desconectar de la corriente eléctrica el ordenador mientras se está trabajando con él o la eliminación de documentos o datos de un archivo, hasta la utilización de los más complejos programas lógicos destructivos (crash programs), sumamente riesgosos para los sistemas, por su posibilidad de destruir gran cantidad de datos en un tiempo mínimo.

Estos programas destructivos, utilizan distintas técnicas de sabotaje, muchas veces, en forma combinada. Sin pretender realizar una clasificación rigurosa de estos métodos de destrucción lógica, se pueden distinguir:

Bombas lógicas (time bombs): En esta modalidad, la actividad destructiva del programa comienza tras un plazo, sea por el mero transcurso del tiempo (por ejemplo a los dos meses o en una fecha o a una hora determinada), o por la aparición de determinada señal (que puede aparecer o puede no aparecer), como la presencia de un dato, de un código, o cualquier mandato que, de acuerdo a lo determinado por el programador, es identificado por el programa como la señal para empezar a actuar. La jurisprudencia francesa registra un ejemplo de este tipo de casos. Un empleado programó el sistema de tal forma que los ficheros de la empresa se destruirían automáticamente si su nombre era borrado de la lista de empleados de la empresa.

Otra modalidad que actúa sobre los programas de aplicación es el llamado **cáncer de rutinas (cancer routine).** En esta técnica los programas destructivos tienen la particularidad de que se reproducen, por sí mismos, en otros programas, arbitrariamente escogidos.

Una variante perfeccionada de la anterior modalidad es el **virus informático**, que es un programa capaz de multiplicarse por sí mismo y contaminar los otros programas que se hallan en el mismo disco duro donde fue instalado y en los datos y programas contenidos en los distintos discos con los que toma contacto a través de una conexión a la red.

B. **Fraude a través de computadoras**: Estas conductas consisten en la manipulación ilícita, a través de la creación de datos falsos o la alteración de datos o procesos contenidos en sistemas informáticos, realizada con el objeto de obtener ganancias

indebidas. Los distintos métodos para realizar estas conductas se deducen, fácilmente, de la forma de trabajo de un sistema informático:

En primer lugar, es posible alterar datos, omitir ingresar datos verdaderos o introducir datos falsos en un ordenador, siendo un proceso sumamente fácil pues todos tienen acceso a un ordenador en esta época. Esta forma de realización se conoce como manipulación del input.

En segundo lugar, es posible interferir en el correcto procesamiento de la información, alterando el programa o secuencia lógica con el que trabaja el ordenador. Esta modalidad puede ser cometida tanto al modificar los programas originales, como al adicionar al sistema programas especiales que introduce el autor. A diferencia de las manipulaciones del input que, incluso, pueden ser realizadas por personas sin conocimientos especiales de informática, esta modalidad requiere conocimientos técnicos especiales, por tratarse de un proceso más complejo.

Y por último, es posible falsificar el resultado, inicialmente correcto, obtenido por un ordenador: a esta modalidad se la conoce como manipulación del output. Una característica general de este tipo de fraudes, interesante para el análisis jurídico, es que, en la mayoría de los casos detectados, la conducta delictiva es repetida varias veces en el tiempo. Lo que sucede es que, una vez que el autor descubre o genera una laguna o falla en el sistema, tiene la posibilidad de repetir, cuantas veces quiera, la comisión del hecho. Incluso, en los casos de manipulación del programa, la reiteración puede ser automática, realizada por el mismo sistema sin ninguna participación del autor y cada vez que el programa se active. En el ejemplo jurisprudencial citado al hacer referencia a las

manipulaciones en el programa, el autor podría irse de vacaciones, ser despedido de la empresa o incluso morir y el sistema seguiría imputando el pago de sueldos a los empleados ficticios en su cuenta personal.

Una problemática especial plantea la posibilidad de realizar estas conductas a través de los sistemas de teleproceso. Si el sistema informático está conectado a una red de comunicación entre ordenadores, a través de las líneas telefónicas o de cualquiera de los medios de comunicación remota de amplio desarrollo en los últimos años, el autor podría realizar estas conductas sin ni siquiera tener que ingresar a las oficinas donde funciona el sistema, incluso desde su propia casa y con una computadora personal. Aún más, los sistemas de comunicación internacional, permiten que una conducta de este tipo sea realizada en un país y tenga efectos en otro.

Respecto a los objetos sobre los que recae la acción del fraude informático, estos son, generalmente, los datos informáticos relativos a activos o valores. En la mayoría de los casos estos datos representan valores intangibles (Ej.: depósitos monetarios, créditos, etc.), en otros casos, los datos que son objeto del fraude, representan objetos corporales (mercadería, dinero en efectivo, etc.) que obtiene el autor mediante la manipulación del sistema. En las manipulaciones referidas a datos que representan objetos corporales, las pérdidas para la víctima son, generalmente, menores ya que están limitadas por la cantidad de objetos disponibles. En cambio, en la manipulación de datos referida a bienes intangibles, el monto del perjuicio no se limita a la cantidad existente sino que, por el contrario, puede ser creado por el autor.

C. **Estafas electrónicas**: La proliferación de las compras telemáticas permite que aumenten también los casos de estafa. Se trataría en este caso de una dinámica comisiva que cumpliría todos los requisitos del delito de estafa, ya que además del engaño y el "animus defraudandi" existiría un engaño a la persona que compra. No obstante seguiría existiendo una laguna legal en aquellos países cuya legislación no prevea los casos en los que la operación se hace engañando al ordenador.

D. **Copia ilegal de software y espionaje informático**: Se engloban las conductas dirigidas a obtener datos, en forma ilegítima, de un sistema de información. Es común el apoderamiento de datos de investigaciones, listas de clientes, balances, etc. En muchos casos el objeto del apoderamiento es el mismo programa de computación (software) que suele tener un importante valor económico.

E. **Infracción de los derechos de autor**: La interpretación de los conceptos de copia, distribución, cesión y comunicación pública de los programas de ordenador utilizando la red provoca diferencias de criterio a nivel jurisprudencial.

F. **Infracción del copyright de bases de datos**: No existe una protección uniforme de las bases de datos en los países que tienen acceso a internet. El sistema de protección más habitual es el contractual: el propietario del sistema permite que los usuarios hagan "downloads" de los ficheros contenidos en el sistema, pero prohíbe realizar réplicas de la base de datos o la copia masiva de información.

G. **Uso ilegítimo de sistemas informáticos ajenos**: Esta modalidad consiste en la utilización sin autorización de los ordenadores y los programas de un sistema

informático ajeno. Este tipo de conductas es comúnmente cometida por empleados de los sistemas de procesamiento de datos que utilizan los sistemas de las empresas para fines privados y actividades complementarias a su trabajo. En estos supuestos, sólo se produce un perjuicio económico importante para las empresas en los casos de abuso en el ámbito del teleproceso o en los casos en que las empresas deben pagar alquiler por el tiempo de uso del sistema.

H. **Acceso no autorizado**: La corriente reguladora sostiene que el uso ilegítimo de passwords y la entrada en un sistema informático sin la autorización del propietario debe quedar tipificado como un delito, puesto que el bien jurídico que acostumbra a protegerse con la contraseña es lo suficientemente importante para que el daño producido sea grave.

I. **Delitos informáticos contra la privacidad**: Grupo de conductas que de alguna manera pueden afectar la esfera de privacidad del ciudadano mediante la acumulación, archivo y divulgación indebida de datos contenidos en sistemas informáticos. Esta tipificación se refiere a quien, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o cualquier otro tipo de archivo o registro público o privado.

J. **Interceptación de e-mail**: En este caso se propone una ampliación de los preceptos que castigan la violación de correspondencia, y la interceptación de telecomunicaciones, de forma que la lectura de un mensaje electrónico ajeno revista la misma gravedad.

K. **Pornografía infantil**: La distribución de pornografía infantil por todo el mundo a través del internet está en aumento. El problema se agrava al aparecer nuevas tecnologías, como la criptografía, que sirve para esconder pornografía y demás material ofensivo que se transmita o archive.

b. Según su fin u objetivo

En esta categoría, se enmarcan las conductas criminales que van dirigidas contra los equipos, 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.).

c. Según actividades delictivas graves

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

Terrorismo: Mensajes anónimos aprovechados por grupos terroristas para remitirse consignas y planes de actuación a nivel internacional. La existencia de hosts que ocultan la identidad del remitente, convirtiendo el mensaje en anónimo ha podido ser aprovechado por grupos terroristas para remitirse consignas y planes de actuación a nivel internacional.

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

Espionaje industrial: Accesos no autorizados a sistemas informáticos de grandes compañías, usurpando diseños industriales, fórmulas, sistemas de fabricación y know how estratégico que posteriormente ha sido aprovechado en empresas competidoras o ha sido objeto de una divulgación no autorizada.

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.

3.4. Sobre los contratos informáticos

No pueden caber dudas de que los contratos celebrados por medios informáticos son válidos, ya que el ordenamiento civil establece la voluntad de ambas personas para realizar el mismo.

En la presente investigación se habla mucho de los problemas de los sistemas de información en red, y se trata de establecer que la legislación guatemalteca no necesita

solamente regular lo penal, sino que puede abarcar otros campos como lo civil y mercantil para prevenir situaciones penales, ya que estas otras materias pueden crear mecanismos legales de defensa ante hechos ilícitos de otras personas.

El contrato informático se puede definir como: "En sentido amplio u objetivo, abarca todos aquellos convenios cuyo objeto sea un bien o servicio informático, independientemente de la vía por la que se celebren. En sentido restringido o formal, son aquellos contratos cuyo perfeccionamiento se da por vía informática, indiferentemente de cuál sea su objeto. A estos últimos se les conoce también, propiamente, como contratos electrónicos."[21]

En definitiva, la contratación electrónica o por medios electrónicos se puede definir como aquélla que, con independencia de cuál sea su objeto, pudiendo ser también la informática, se realiza a través o con ayuda de medios electrónicos, siendo estos de distinta naturaleza. En esta categoría de contratos, las partes manifiestan o expresan su consentimiento en forma digital y dan aceptación del Artículo 1517 del Código Civil de Guatemala, salvo que la ley exija una determinada forma para estos, en cuyo caso el contrato no podrá celebrarse por medios informáticos, pues se correrá el riesgo de que sea nulo (si la forma contractual es solemne absoluta) o de que por el hecho de ser virtual no pueda en determinado momento utilizarse como medio probatorio.

La formación de este contrato consensual (pues basta el mero acuerdo de voluntades) no difiere de la formación de los contratos en general; esto es, requiere de una oferta y

[21] Davara Rodríguez, Miguel Ángel. **Derecho informático** Pág. 57

aceptación, que serán manifestaciones de voluntad expresadas por medios digitales entre personas que están comunicadas a través de sistemas informáticos interconectados. La manifestación se realiza mediante un simple clic del mouse.

Así, si el negocio se concreta por operaciones on line (comunicación interactiva o simultánea), se entenderá que es un contrato entre presentes pues la aceptación es inmediatamente conocida; en cambio, será entre ausentes si la aceptación no es emitida on line o requiere de una confirmación posterior por el oferente, enviada por otro medio (sea fax, teléfono o correo electrónico).

Esta contratación a través de medios informáticos ha dado lugar a lo que se llama el negocio virtual; que consiste en la producción, distribución, comercialización, venta o entrega de bienes y servicios por medios electrónicos y que dentro del ámbito comercial en Guatemala, aun cuando no existe una legislación idónea para ello se da.

Se clasifica a los contratos informáticos de la siguiente manera:

A. **Por el objeto:**

a) Contrato de hardware (la parte física del sistema informático);
b) Contrato de software (debiendo diferenciarse si se trata de un software de base o sistema o si se trata de un software de utilidad o de aplicación para el usuario);
c) Contrato de instalación llave en mano (aquí se incluyen tanto el hardware como el software, así como determinados servicios de mantenimiento y de formación del usuario);

d) Contrato de servicios auxiliares (el mantenimiento de equipos o la formación de personas que van a utilizar la aplicación).

B. **Por el negocio jurídico en**:

a) De venta (el vendedor se obliga a entregar una cosa determinada, un bien informático y la otra parte a pagar un precio cierto, incluyéndose también a los servicios en esta categoría);

b) De alquiler (el arrendamiento sobre los bienes informáticos es un arrendamiento tipo de los regulados en el Código Civil, caracterizado porque el suministrador se obliga a dar al usuario el goce o uso del bien durante un tiempo determinado y por un precio cierto);

c) De mantenimiento (puede ser tanto de equipos como de programas o inclusive, mantenimiento integral en el que se puede incluir un servicio de formación, asesoramiento y consulta);

d) De prestación de servicios (se incluye análisis, especificaciones, horas máquina, tiempo compartido, programas, etc.);

e) De ejecución de obra;

f) De préstamo (caracterizado porque una parte entrega a otra el bien informático para que lo use durante un tiempo determinado y lo devuelva una vez cumplido ese tiempo);

g) De comodato (consistente en un tipo de contrato de préstamo en el que el suministrador transfiere el uso del bien informático prestado);

h) De depósito (se constituye desde que una persona recibe una cosa ajena con la obligación de guardarla y restituirla, siendo un contrato gratuito, salvo pacto en contrario);

i) Licencia de uso (es el contrato en virtud del cual el titular de los derechos de explotación de un programa de ordenador autoriza a otro a utilizar el programa conservando el cedente la propiedad del mismo);

j) Adaptación de un software producto (se trata de la contratación de una licencia de uso de un producto estándar que habrá de adaptarse a las necesidades del usuario);

k) "Escrow" o garantía de acceso al código fuente (son aquellos que tienen por objeto garantizar al usuario el acceso a un programa fuente en el caso de que desaparezca la empresa titular de los derechos de propiedad intelectual);

l) Contrato de distribución de información (consiste en la comercialización de la base de datos, durante un cierto periodo de tiempo a cambio de un precio, lo que origina la obligación por parte del titular de la base de aportar los datos que deben hacerse accesibles a los futuros usuarios, en una forma adecuada para su tratamiento por el equipo informático del distribuidor, y ceder a este último, en exclusiva o compartidos con otros distribuidores, los derechos de explotación);

m) Contrato de suministro (mediante este contrato el usuario puede acceder a las bases de datos del distribuidor);

n) Contrato de información (el titular de una base de datos vende a otro una copia de ésta con la posibilidad que el adquirente, a su vez, pueda no sólo usarla sino mezclarla con otras propias para su posterior comercialización).

C. **Los contratos complejos**: (aquellos que contemplan los sistemas informáticos en su integridad). Modalidades de esta especie:

a) Contrato parcial y global de servicios informáticos (es la subcontratación de todo o de parte del trabajo informático, mediante un contrato con una empresa externa que

se integra en la estrategia de la empresa y busca diseñar una solución a los problemas existentes, donde también se incluyen los auditores informáticos).

b) Contrato de respaldo o "back up" (la finalidad es asegurar el mantenimiento de la actividad empresarial en el caso que circunstancias previstas pero inevitables impidan que siga funcionando el sistema informático poniendo a disposición de la empresa, dentro de los límites del contrato, los medios informáticos para que pueda continuar el proceso).

En términos generales los contratos más comunes en internet son las compras de programas informáticos (software), hardware, fonogramas comerciales, música, libros, acciones, servicios de post-venta y turismo.

Así también, los riesgos de la contratación informática se presentan y vinculan con la falta de seguridad que puede existir, la que se origina en las demoras o faltas de envío de la mercadería contratada, la inalterabilidad de los contenidos de la oferta, contraoferta y aceptaciones que se pueden modificar si son interceptadas, la falta de identidad de los contratantes y su eventual incapacidad.

En este contexto la firma y los certificados digitales resultan herramientas de inestimable valor desde el momento en que los contratos se realizan on-line (a través de la internet); es decir, sin la presencia física de las partes y frente a la utilización de las nuevas tecnologías (dando lugar a la comisión de los delitos informáticos), que atentan contra la información como bien jurídico de naturaleza colectiva o macrosocial.

En definitiva, la firma digital se presenta como un instrumento de seguridad y confidencialidad de las actividades que se producen en el curso de la interacción humana en todos sus ámbitos y que dependen de los sistemas informáticos (transporte, comercio, sistema financiero, gestión gubernamental, arte, ciencia, relaciones laborales, tecnología, etc.).

No es posible soslayar que la mayoría de los casos de los contratos informáticos tienen por objeto la adquisición de cosas muebles o de servicios para el consumo final o beneficio del propio adquirente, de su grupo familiar o social. En otras palabras, el adquirente de la cosa o servicio es un verdadero consumidor; que en consecuencia, está amparado por la ley, la que dispone que la interpretación del contrato deberá ser hecha en el sentido que más lo favorezca a éste.

3.5. Análisis del derecho comparado en relación al ciberdelito

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

Respecto a la definición de la Organización para la Cooperación Económica y el Desarrollo, define al delito informático como: "Cualquier conducta ilegal, no ética o no

autorizada que involucra el procesamiento automático de datos y/o la transmisión de datos".[22]

En cuanto a la Comisión Europea, se centró en un concepto amplio de delito informático, al indicar que es cualquier delito que de alguna manera implique el uso de la tecnología de la información.

No se puede establecer que en Guatemala exista una definición propia de lo que se considera delito informático; pues a pesar que existen ya en vigencia tres leyes que tratan de normar lo relacionado a algunas actividades ilícitas que se pueden cometer por medios informáticos (Código Penal, Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas, Ley de Acceso a la Información Pública), no se establece una definición concreta de delito informático, demostrando una vez más la falta de una legislación concreta y amplia que reúna todo lo concerniente al delito cibernético.

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

[22] Hugo Vizcardo, Silfredo. **Delitos informáticos**. Pág. 95

tal como lo es el caso de Guatemala en el último aspecto en donde existen empresas de información de red denominadas TransUnión e Infornet.

Cabe indicar aquí que no son los grandes sistemas de información los que afectan la vida privada sino la manipulación o el consentimiento de ello, por parte de individuos poco conscientes e irresponsables en el manejo de los datos que dichos sistemas contienen. La humanidad no está frente al peligro de la informática sino frente a la posibilidad real de que individuos o grupos sin escrúpulos, con aspiraciones de obtener el poder que la información puede conferirles, la utilicen para satisfacer sus propios intereses, a expensas de las libertades individuales y en detrimento de las personas. Asimismo, la amenaza futura será directamente proporcional a los adelantos de las tecnologías informáticas.

"La protección de los sistemas informáticos puede abordarse tanto desde una perspectiva penal como de una perspectiva civil o comercial, e incluso de derecho administrativo. Estas distintas medidas de protección no tienen porque ser excluyentes unas de otras, sino que, por el contrario, éstas deben estar estrechamente vinculadas. Por eso, dadas las características de esta problemática sólo a través de una protección global, desde los distintos sectores del ordenamiento jurídico, es posible alcanzar una cierta eficacia en la defensa de los ataques a los sistemas informáticos".[23]

Ahora bien, las normas jurídicas que se han puesto en vigor en otros países están dirigidas a proteger la utilización abusiva de la información reunida y procesada mediante el uso de computadoras. Desde hace algún tiempo algunos países han hecho todo lo

[23] Osorio Meléndez, A. Hugo **.Políticas de información y derecho. Estudio comparativo.** Pág. 54.

posible para incluir dentro de la ley, la conducta punible penalmente, como el acceso ilegal a sistemas de cómputo o el mantenimiento ilegal de tales accesos, la difusión de virus o la interceptación de mensajes informáticos.

Las personas que cometen los delitos informáticos son aquéllas 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, aun cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos.

En síntesis, es destacable que la delincuencia informática se apoya en el delito instrumentado por el uso de los equipos computarizados a través de redes telemáticas y la interconexión de estos, aunque no son el único medio. Las ventajas y las necesidades del flujo nacional e internacional de datos, que aumenta de modo acelerado aun en países latinoamericanos, conlleva también 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 encargadas de las investigaciones y los funcionarios judiciales.

En el contexto internacional, son pocos los países que cuentan con una legislación apropiada. Entre ellos se destacan: Estados Unidos de América, 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 de América

Este país adoptó en 1994 el Acta Federal de Abuso Computacional que modificó el Acta de Fraude y Abuso Computacional de 1986; con la finalidad de eliminar los argumentos técnicamente avanzados sobre a qué debiese considerársele un virus, un gusano, un caballo de troya y en qué 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 equipo computarizado o red informática.

En julio de 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 y entre empresas y consumidores.

b. Alemania

Este país sancionó en 1986 la Ley contra la Criminalidad Económica, que contempla los siguientes delitos: Espionaje de datos, estafa informática, alteración de datos y sabotaje informático.

c. Austria

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

d. Gran Bretaña

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

e. Holanda

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

- El hacking.

- El preacking (utilización de servicios de telecomunicaciones evitando el pago total o parcial de dicho servicio).
- La ingeniería social (arte de convencer a la gente de entregar información que en circunstancias normales no entregaría).
- La distribución de virus.

f. Francia

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

- Intromisión fraudulenta que suprima o modifique datos.
- Conducta intencional en la violación de derechos a terceros que haya impedido o alterado el funcionamiento de un sistema de procesamiento automatizado de datos.
- 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.
- Supresión o modificación de datos contenidos en el sistema, o bien en la alteración del funcionamiento del sistema (sabotaje).

g. España

En el 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:

- La 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.

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

- 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.

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

- 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.
- Conducta maliciosa tendiente a la destrucción o inutilización de un sistema de tratamiento de información o de sus partes componentes o que dicha conducta impida, obstaculice o modifique su funcionamiento.
- Conducta maliciosa que altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información.

La legislación guatemalteca, como ya se mencionó, cuenta con tres cuerpos normativos que hacen referencia a ciertas actividades ilícitas que pueden realizarse mediante el ciberespacio:

-Código Penal, destrucción de registros electrónicos, alteración de programas, reproducción de instrucciones o programas de computación, registros prohibidos, manipulación de información, uso de información, programas destructivos

-Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas, que hace referencia a las actividades ilícitas por parte de los certificadores de operaciones electrónicas.

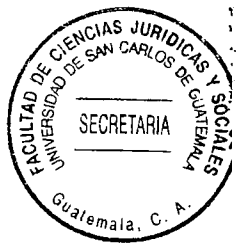
-Ley de Acceso a la Información Pública, uso y difusión de la información, comercialización de datos personales, alteración o destrucción de información en archivos.

Luego de lo expuesto, se puede determinar que la legislación guatemalteca es insuficiente; pues no permite encuadrar todas las actividades ilícitas que se pueden realizar por medio del ciberespacio; establece ciertas actividades que tienen relación con los delitos informáticos, pero en definitiva no encuadra claramente todos los delitos informáticos, y tampoco hace referencia a actividades propias de las redes sociales, o portales electrónicos; la legislación guatemalteca se limita a enmarcar los delitos informáticos, como aquellas actividades relacionadas con el manejo de datos y de archivos informáticos.

Asimismo, la legislación guatemalteca en esta materia, tiene como principal característica la no codificación; pues cuenta con diversos cuerpos normativos que tratan de regular la informática, en comparación con las demás legislaciones expuestas, en las que se puede observar que cuentan con una ley específica sobre la materia, pues debido a la

importancia que la informática tiene, los legisladores en otros países han optado por crear una propia legislación sobre la informática.

La legislación referente a los delitos informáticos, debe ser una legislación que permita encuadrar distintas actividades en un solo tipo penal, pues estas actividades delictivas no son siempre en un solo sentido o bajo un solo móvil; las actividades cibernéticas día a día van cambiando en cuanto a su forma de comisión, y la propia evolución de los sistemas de red hace realmente conflictivo crear un tipo penal que encuadre una sola actividad o que sea tan específica que se vea desfasada al día siguiente de su creación; por lo que se determina que la legislación en materia informática tiene que ser positiva y que tenga la capacidad de ir adecuándose día a día a las distintas sociedades.


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

CAPÍTULO IV

4. Análisis sobre la postura del Estado de Guatemala frente al ciberdelito

4.1. De los compromisos adquiridos a nivel internacional

El Manual de Naciones Unidas para la Prevención y Control de Delitos Informáticos estipula: "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".[24]

Por otra parte además, la ONU resume los problemas que rodean a la cooperación internacional en el área de los delitos informáticos:

- Falta de acuerdos globales acerca de qué tipo de conductas deben constituir delitos informáticos.
- Ausencia de acuerdos globales en la definición legal de dichas conductas delictivas.
- Falta de especialización de las policías, fiscales y otros funcionarios judiciales en el campo de los delitos informáticos.
- Falta de armonización entre las diferentes leyes procesales nacionales acerca de la investigación de los delitos informáticos.

[24] http://www.uncjin.org/Documents/congr10/10s.pdf **prevención del delito y tratamiento del delincuente** (Guatemala, 23 de enero de 2011)

-Carácter transnacional de muchos delitos cometidos mediante el uso de computadoras.

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

"Desde siempre, la relación entre internet y el derecho ha sido difícil, no sólo por la evidente trascendencia del nuevo formato de comunicación que supone la instauración de internet, con amplia difusión a un grupo también amplísimo y variado de destinatarios, con las ventajas e inconvenientes que ya de por sí conlleva, sino porque, de la misma forma, se convierte en un evidente campo de cultivo para las más variadas conductas ilícitas, y ello no sólo en el ámbito penal".[25]

Ante esto Guatemala, no ha adquirido compromisos respecto del ciberdelito o delitos informáticos; se puede decir que cuenta con una legislación en materia de tipificación de delitos informáticos, la cual se encuentra incorporada en el Código Penal; pero el patrón común que se ve en la sanción de este tipo de delitos, es que las penas impuestas son muy insignificantes, van desde los seis meses hasta los cuatro años en algunas casos de dos años; si se toma en cuenta que son delitos que dejan pérdidas millonarias; además, no se incorporan otros delitos informáticos, como es el sabotaje informático, y la interceptación de datos; sin embargo, no es sólo característica de Guatemala, pues en otros países se repite el mismo patrón.

En materia de derecho internacional es necesario mencionar que existe el Convenio de Ciberdelincuencia del Consejo de Europa; firmado en Budapest el 23 de noviembre de 2001, ratificado por Albania, Croacia, Estonia, Hungría, Lituania, Rumania, Eslovenia y

[25] Cruz de Pablo, José Antonio. **Derecho penal y nuevas tecnologías**. Pág. 11

Macedonia. Surge como consecuencia del desarrollo y utilización cada vez mayor de las tecnologías de la información y la comunicación, así como de la necesidad de aplicar una política penal común, encaminada a proteger a la sociedad frente a la ciberdelincuencia, adoptando la legislación adecuada y manteniendo una política de cooperación internacional.

El Convenio señala los delitos informáticos en los siguientes grupos, y define los tipos penales que han de considerarse para cada uno ellos:

- Delitos contra la confidencialidad, la integridad, y la disponibilidad de los datos y sistemas informáticos.
- Delitos informáticos.
- Delitos relacionados con el contenido.
- Delitos relacionados con infracciones de la propiedad intelectual y derechos afines.
- Posteriormente, en 2003, se promulgó la firma del Protocolo Adicional al Convenio de Ciberdelincuencia del Consejo de Europa para criminalizar actos de racismo y xenofobia.

Las conductas consideradas en el Convenio de Ciberdelincuencia del Consejo de Europa no están tipificadas de igual manera en el Código Penal español; y se menciona esto pues a lo largo de la historia se ha observado cómo la legislación que utiliza Guatemala y el resto de Latinoamérica como ejemplo o referencia es la legislación española; por lo que resulta interesante y apropiado establecer que los tipos penales relacionados a la informática que se encuentran en el ordenamiento español son:

De las amenazas, de los delitos de exhibicionismo y provocación sexual, de los delitos relativos a la prostitución y la corrupción de menores, del descubrimiento y revelación de secretos, de la calumnia, de la injuria, de las estafas, de las defraudaciones de fluido eléctrico, de los daños, de los delitos relativos a la propiedad intelectual, de los delitos relativos a la propiedad industrial, de los delitos relativos al mercado y a los consumidores (descubrimiento de secreto de empresa), de los delitos relativos a las falsedades documentales y de los delitos contra la comunidad internacional (apología del racismo y la xenofobia).

Así pues, puede establecerse que existen a nivel internacional distintos convenios y proyectos que hacen referencia la legislación del cieberdelito; pero Guatemala no ha ratificado o suscrito ninguno de ellos, y esto es simplemente reflejo de la importancia que ha dado el Estado de Guatemala al tema del ciberdelito.

4.2. Del análisis de la necesidad de creación de la legislación específica para Guatemala

En Guatemala, la inexistencia de una ley informática imposibilita que la persecución y castigo de los autores de delitos informáticos sea efectiva. Aunado a esto las autoridades (Policía Nacional Civil, Ministerio Público, Órgano Judicial) no poseen el nivel de experiencia requerido en estas áreas ni la capacidad requerida para desarrollar actividades de investigación, persecución y recopilación de pruebas digitales y electrónicas. Por lo que todo tipo de acción contra los delincuentes informáticos queda prácticamente en manos de la organización que descubre un delito y; el tipo de

penalización puede considerase administrativa por no lograr tipificarlos dentro de los ya establecidos tipos penales (si el delito proviene de fuentes internas).

Si se trata de delitos cometidos directamente por particulares, la situación se agrava mucho más, debido a que los resultados de persecución son demasiado escasos y pobres. En este rubro cabe mencionar lo que pasa por ejemplo con un delito que aun cuando lo prevé la legislación guatemalteca en el Código Penal, con la figura de piratería, el mismo constituye un delito informático; siendo preocupante que aunque el delito se comete en muchas calles de Guatemala e incluso en locales, el mismo no es atacado; puesto que en muy contadas ocasiones se han realizado allanamientos para determinar los sistemas de información que fortalecen este tipo de ilegalidades; y mucho menos se han logrado condenas, lo cual perjudica a un sinfín de personas y empresas y hasta la economía de Guatemala.

Por eso es de suma importancia la creación de legislación específica sobre delitos informáticos o del ciberdelito; debido a que el impacto se puede observar de manera general; por ejemplo: hoy día las redes de información virtual han crecido de manera asombrosa, dando lugar a una gran cantidad de actividades tales como: compras, pago de servicios, negocios y hasta consultas médicas, entre otras.

Esto quiere decir entonces que así como se amplía la cobertura de internet, tal como sucede en Guatemala, en donde actualmente se puede hacer uso del mismo a través de un modem en cualquier parte del territorio nacional; asimismo va aumentando el uso indebido de esta tecnología.

Los denominados delincuentes cibernéticos se mantienen en contacto constate con el mundo virtual; incurriendo en delitos tales como el acceso sin autorización o piratería informática, el fraude, el sabotaje informático, la trata de niños con fines pornográficos, etc.

De esa cuenta los delincuentes de la informática son tan diversos como sus delitos; puede tratarse de estudiantes, terroristas o figuras del crimen organizado; siendo estos últimos el grupo de más alto impacto actual en Guatemala. Estos delincuentes pueden pasar desapercibidos a través de las fronteras virtuales, ocultarse tras incontables enlaces o simplemente desvanecerse sin dejar ningún documento de rastro. Pueden despachar directamente las comunicaciones o esconder pruebas delictivas en paraísos informáticos o sea, en países que carecen de leyes o experiencia para seguirles la pista, tal y como sucede para un país como Guatemala, el cual si bien es cierto, contempla figuras penales respecto al tema en discusión las mismas no suplen efectivamente primero la figura penal establecida y segundo mucho menos una figura de índole informático.

En Guatemala, recientemente en abril de 2011 se publicó la detención de una banda de delincuentes que se dedicaban a la clonación de tarjetas bancarias; que afectaban los derechos de los cuentahabientes, pero se le encuadró en el tipo penal de estafa establecido en el Código Penal; por no existir la figura referente a los delitos informáticos en los cuales incurrieron y que pudieron agregarse dentro de los procesos que se hayan iniciado, con la peculiaridad de que todos los sindicados eran empleados de un banco del sistema.

En 1990, se supo por primera vez en Europa de un caso en que se usó un virus con fines ilícitos; cuando la comunidad de investigación médica se vio amenazada con un virus que iría destruyendo datos paulatinamente si no se pagaba un rescate por la desactivación del mismo.

"Los delincuentes cibernéticos al acecho también usan el correo electrónico para enviar mensajes amenazantes especialmente a las mujeres, se calcula que unas 200.000 personas acosan a alguien cada año".[26] Los delincuentes también han utilizado el correo electrónico y los chat o salas de conversación por internet para buscar presas vulnerables. Por ejemplo, los aficionados a la pedofilia se han ganado la confianza de niños online y luego concertado citas reales con ellos para explotarlos o secuestrarlos, tal como ha pasado en algunos departamentos de Guatemala.

Así también, es de suma importancia establecer una legislación específica sobre las acciones ilícitas por medio de redes de información por el impacto a nivel social que esto provoca; ya que la proliferación de los delitos informáticos ha hecho que la sociedad sea cada vez más escéptica a la utilización de tecnologías de la información, las cuales pueden ser de mucho beneficio para la sociedad en general. Este hecho puede obstaculizar el desarrollo de nuevas formas de hacer negocios, por ejemplo el comercio electrónico puede verse afectado por la falta de apoyo de la sociedad en general, aun cuando Guatemala es considerada un país con poco avance en ese tipo de tecnología.

---

[26] Jenson, Bárbara. **Acecho cibernético: delito, represión y responsabilidad personal en el mundo online.** Pág. 13

Asimismo, se observa que las empresas que poseen activos informáticos importantes, son cada vez más celosas y exigentes en la contratación de personal para trabajar en estas áreas, pudiendo afectar en forma positiva o negativa a la sociedad laboral en estos tiempos, tomando en cuenta que Guatemala se encuentra ante situaciones graves económicas y que perjudican al ciudadano. Aquellas personas que no poseen los conocimientos informáticos básicos, son más vulnerables a ser víctimas de un delito, que aquellos que si los poseen. En vista de lo anterior el porcentaje de personas que no conocen nada de informática (por lo general personas de escasos recursos económicos) pueden ser engañadas si en un momento dado tienen acceso a recursos tecnológicos y no han sido asesoradas adecuadamente para la utilización de tecnologías como la internet, correo electrónico, etc.

4.3. Del fortalecimiento de la legislación respecto a los sistemas de información y el respeto del derecho a la intimidad y de la protección de los datos personales

"El derecho a la intimidad abarca aquello que se considera más propio y oculto del ser humano entendiéndose por propio y oculto la información que mantiene para sí mismo. Pero es insoslayable que el contacto permanente del ser humano con sus semejantes al interior de la sociedad a la que pertenece, así como todos aquellos avances tecnológicos que han venido desarrollándose en la sociedad, han comenzado a transgredir aquellos ámbitos que forman parte de la intimidad del ser humano".[27]

[27] García González, Aristeo. **El derecho a la intimidad desde una perspectiva constitucional: equilibrio, alcances, límites y mecanismos de defensa.** Pág. 94

"La intimidad, marcada por un matiz individualista, era la facultad destinada a salvaguardar un determinado espacio con carácter exclusivo, y que consistía en un derecho del individuo a la soledad y a tener una esfera reservada en la cual desenvolver su vida sin que la indiscreción ajena tenga acceso a ella".[28]

"Al igual que el resto de los derechos humanos, el derecho a la intimidad ha tenido su historicidad y positividad, y se ha consagrado con la modernidad, la intimidad de la persona ha encontrado su justificación y fundamento en el derecho".[29] Un derecho tal como ha sido reconocido por las normas puede justificarse por su capacidad de promover ciertos bienes jurídicos básicos para los ciudadanos: como es la libertad, la igualdad, la seguridad y otros semejantes. "Por lo que desde esta perspectiva puede justificarse la intimidad como un medio para promover la libertad individual, a lo que se le denomina el goce pacífico y la independencia privada, mientras que la única libertad que merece este nombre es la de buscar nuestro propio bien a nuestra propia manera".[30]

Sin embargo, la intimidad como una disciplina jurídica ha perdido su carácter exclusivo individual y privado, para asumir progresivamente una significación pública y colectiva, consecuencia del cauce tecnológico. "Por otra parte, en el mismo sentido, debe de señalarse que la privacidad no implica sencillamente la falta de información sobre nosotros por parte de los demás, sino más bien el control que tenemos sobre las informaciones que nos conciernen".[31]

---

[28] Battle, Georgina. **El derecho a la intimidad privada y su regulación**. Pág. 191.
[29] García González, Aristeo. **Ob. Cit**. Pág. 8
[30] Stuart Mill, John. **Sobre la libertad**. Pág. 126
[31] Pérez Luño, A. **Derechos humanos, estado de derecho y Constitución**. Pág. 334

Consecuentemente, frente a una actual sociedad de la información, resulta insuficiente hoy concebir a la intimidad como una derecho garantista (estatus negativo) de defensa frente a cualquier invasión indebida de la esfera privada, sin contemplarla al mismo tiempo, como un derecho activo de control (estatus positivo) sobre el flujo de informaciones que afectan a cada sujeto.

La propia noción de intimidad o privacidad es una categoría cultural, social e histórica. Por lo que ahora este concepto ha pasado de una concepción cerrada y estática de la intimidad a otra abierta y dinámica. Puesto que ahora se contempla la posibilidad de conocer, acceder y controlar las informaciones concernientes a cada persona.

En la modernidad, el derecho a la intimidad, visto como el más reciente derecho individual relativo a la libertad, ha variado profundamente, fruto de la evolución tecnológica. Por tanto, ha sido necesario ampliar su ámbito de protección, así como el establecimiento de nuevos instrumentos de tutela jurídica.

Consecuentemente, una teoría de la intimidad encerrada en sí misma no sólo sería incapaz de explicar satisfactoriamente la función de este derecho en la experiencia política, científica y cultural del presente, sino, incluso, sería inútil (o, en el peor de los casos, deformadora) la formulación de su concepto.

"Al tratarse de un derecho con un carácter abierto y dinámico que está frente a una sociedad donde la informática se ha convertido en el símbolo emblemático de la cultura actual, se señala acertadamente que el control electrónico de los documentos de identificación, el proceso informatizado de datos fiscales, el registro de crédito, así como

de las reservas de viajes, representan muestras conocidas de la omnipresente vigilancia informática de la existencia habitual de la persona. Por lo que la vida individual y social corre el riesgo de hallarse sometida a un juicio universal permanente".[32]

Cada ciudadano fichado en un banco de datos se halla expuesto a una vigilancia continua e inadvertida que afecta potencialmente incluso los aspectos más sensibles de su vida privada, aquellos que en épocas anteriores quedaban fuera de todo control, por su variedad y multiplicidad; y que hoy, además de tomar conciencia de ello, comienzan a exigir un reconocimiento sobre el uso y control de sus datos, tal como sucede para los guatemaltecos por medio de empresas como Infornet y Trans Unión.

"Pero por otra parte la protección de la intimidad frente a la informática no significa impedir el proceso electrónico de informaciones, necesarias en el funcionamiento de cualquier Estado moderno, sino el aseguramiento de un uso democrático de la información".[33]

Antes de haberse reconocido expresamente el derecho a la intimidad como derecho unitario, sólo se reconocían y protegían en el ámbito constitucional manifestaciones concretas de la intimidad; tales como el derecho a la inviolabilidad de domicilio y de las comunicaciones, así como el secreto a la correspondencia; hoy, las nuevas tecnologías, al posibilitar la racionalización, simplificación, celeridad y seguridad de las prácticas administrativas y de recopilación de datos, se presentan como una exigencia inaplazable de regulación, que cualquier Estado debe tener en cuenta.

---

[32] Frosini, Vittorio. **Cibernética, derecho y sociedad.** Pág. 178
[33] Pérez Luño, A. **Ob. Cit**. Pág. 345

Así, en una primera aproximación, cabe señalar que los datos de toda persona deben ser objeto de protección para que estos puedan ser tratados o elaborados, y finalmente ser convertidos en información; y en consecuencia, sólo ser utilizados para los fines y por las personas autorizadas, de ahí la necesidad de formular una correcta legislación para Guatemala que abarque todos los preceptos necesarios.

Con base en lo anterior, conviene iniciar el estudio de la protección de datos, desde el primer desafío de las nuevas tecnologías de la información con respecto a la recolección, procesamiento y transmisión de datos personales. Dentro de esta base, el concepto de la intimidad, en el contexto de la sociedad computarizada, concede derechos a los individuos respecto de sus datos personales que son objeto de tratamiento automatizado, e impone obligaciones y deberes de aquellos que controlan y tienen acceso a los ficheros.

4.4. Análisis del resultado del trabajo de campo

El trabajo de campo consistió en un cuestionario de cinco preguntas relacionadas a los delitos informáticos, actividades ilícitas que se cometen en la red y lo más importante, sobre el derecho a la intimidad y datos privados y personales.

El referido cuestionario fue respondido por cincuenta estudiantes de la Facultad de Ciencias Jurídicas y Sociales de la Universidad de San Carlos de Guatemala, siendo el análisis de las respuestas el siguiente:

La perspectiva del trabajo de campo desarrollado permite dar a conocer que la población en general desconoce muchos aspectos sobre el ciberdelito o delitos informáticos; debido

a circunstancias tales como, que en la actualidad la mayoría de la población en Guatemala, cuenta con acceso a sistemas de información en red y al internet sin reserva alguna.

Además, se considera que actualmente sí se violenta el derecho a la seguridad y dignidad de las personas por medio de algunos sistemas de información en red que tienen funciones en Guatemala y lo peor es que se encuentran autorizados bajo la fachada de actividades de apoyo en información; pero que afectan los intereses de los guatemaltecos. Respecto a ese tipo de violación, la mayoría se refirieron a las empresas Infornet y Trans Unión, así como en su momento relacionaron a otras empresas denominadas o con los títulos de Limpiamos su Crédito.

Por otro lado, es evidente que la población guatemalteca no tiene la confianza necesaria en la justicia; debido a que entienden que la problemática del acceso y efectividad son evidentes en todos los campos y mucho más en el campo de la informática, en la cual las instituciones del sistema de justicia tienen muy poca capacidad tanto humana como tecnológica para combatir este tipo de ilícitos.

Así también, existe conciencia de que Guatemala, es un país muy vulnerable en relación a delitos en esta materia, pero anteponen que ese tipo de ilícitos se dan debido a la falta de atención del Estado, aun cuando algunos de los entrevistados manifestaron que existen proyectos de ley propuestos en el Congreso de la República respecto a delitos informáticos, pero que el contexto de los mismos se encuentra muy alejado de la realidad y que lejos de ser un apoyo sería una limitación, considerando que algunos aspectos serían imposibles de tipificar.

Otro aspecto relevante es que se considera que la forma principal por la cual se dan en Guatemala este tipo de delitos es por medio de conexiones a internet; seguido de las acciones de empleados dentro de empresas que de alguna manera manejan información de tipo confidencial o en las cuales su actividad como tal les permite tener acceso a distintos tipos de información.

Por último pero no menos importante, se estableció que el principal ataque en este tipo de ilícitos es por medio del ingreso ilegal a los sistemas de información; lo cual da a entender que no existen los medios idóneos de conocimiento para defender este tipo de información; considerando posteriormente que los abusos por parte de los empleados en relación al manejo de la información es la segunda forma más común de este tipo de ataques.

Todo lo expuesto, permite determinar que en Guatemala realmente existe la necesidad latente de normar lo concerniente al ciberdelito, y puede establecerse que existe falta de capacidad por parte del Estado en cuanto no existe la aptitud para poder crear esta normativa, pues la mayoría de instituciones desconocen en sí que tan afectadas se ven por la comisión de estas actividades ilícitas; así también se determina que existe incapacidad en virtud de que el Estado no está al tanto del daño que estas actividades le generan a la sociedad en general, más allá del daño que en algunos casos es irreparable y provocado a las personas individualmente.

El Estado como persona jurídica posee capacidad para ejercitar sus derechos y obligaciones; pero en esta investigación se hace referencia a la falta de capacidad debido

a la falta de aptitud del Estado; es decir que necesita fuentes, fundamentos, presupuestos, estudios entre otras cosas; para poder llevar a cabo su función de desarrollar una legislación adecuada a la materia, o sea, cumplir con su obligación de crear cuerpos normativos que protejan al individuo en su totalidad.

En la actualidad Guatemala no cuenta con la debida legislación que norme lo referente al ciberdelito, entendiendo que delito cibernético es todo comportamiento antijurídico, no ético o no autorizado, relacionado con el proceso automático de datos o trasmisiones de datos; puede así también entenderse como aquella acción, tipificada, antijurídica, culpable, punible, que se realice mediante medios electrónicos o tenga como fin el uso de estos sistemas informáticos.

En el Congreso de la República de Guatemala, actualmente se encuentra la iniciativa de ley número 4055 Ley de Delitos Informáticos, la propuesta fue presentada por el diputado independiente Francisco Contreras y algunos expertos latinoamericanos, que trata sobre la importancia de contrarrestar los ilícitos cibernéticos, la que se puede consultar en los anexos de este informe.

Si bien, en el Código Penal existen algunas figuras relacionadas a los delitos informáticos, éstas no son lo suficientemente amplias para encuadrar todas las actividades ilícitas que atañen al ciberdelito, y tampoco son eficientes o positivas para proteger a la población guatemalteca de todas las actividades delictivas relacionadas a la materia.

Finalmente, cabe aclarar que realmente la falta de legislación referente al ciberdelito no es por falta de capacidad del Estado de Guatemala, sino más bien por la falta de voluntad del

Congreso de la República que por cuestiones políticas no se interesan por la seguridad de la población guatemalteca en lo referente al derecho a la seguridad infomática.

CONCLUSIONES

1. La falta de cultura informática en la que se encuentra la población guatemalteca en la actualidad, ha dado lugar a que las mismas personas por falta de conocimiento realicen actividades ilícitas a través de la red.

2. No existe legislación para encuadrar las diversas actividades ilícitas que se llevan a cabo por medio de la red, en el Código Penal no están tipificados los delitos informáticos en su totalidad y por lo mismo no hay una persecución penal sobre estos.

3. El Congreso de la República de Guatemala no tiene interés en aprobar la Ley de Delitos Informáticos, siendo que ésta es de suma importancia, para resolver los conflictos que trae a la sociedad la cieberdelincuencia.

4. Las empresas que actualmente proporcionan datos personales a través de la red; están violentando derechos constitucionales, tales como el derecho a la intimidad y el respeto a los derechos humanos de las personas.

5. El Estado de Guatemala no cuenta con la capacidad necesaria para brindar seguridad cibernética a la población; que ve violentados sus derechos de seguridad y dignidad, a través del manejo inapropiado de datos personales e información confidencial, de las empresas de información por red.


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

RECOMENDACIONES

1. El Ministerio de Educación debe implementar proyectos educativos sobre las tecnologías y sistemas informáticos, para que se conozcan los alcances de la tecnología, y así evitar que por desconocimiento las personas cometan ilícitos penales.

2. el Congreso de la Republica de Guatemala debe poner atención al anteproyecto 4055 donde se presenta la Ley de Delitos Informáticos, que regulara todo lo relativo a los distintos ilícitos penales que se puedan cometer por la red, y así el Ministerio Público pueda cumplir con su principal función, la persecución penal.

3. El Organismo Ejecutivo, la sociedad civil y demás instituciones sociales deben exigir al Congreso de la República la aprobación de la Ley de Delitos Informáticos, ya que los ciberdelitos representan un riesgo no sólo para el comercio internacional sino para la seguridad nacional y economía del país.

4. La Procuraduría General de la Nación como representante del Estado de Guatemala, debe denunciar a las empresas que actualmente proporcionan datos a través de la red; por la violación que hacen a los derechos constitucionales de seguridad e intimidad, pues sólo así se protege a la población de estas actividades que ocasionan daños morales y económicos a las personas.

5. El Estado de Guatemala debe demostrar su capacidad e intención de combatir los ciberdelitos, que afectan a particulares y a la economía de Guatemala, al lograr poner en vigencia el anteproyecto de ley presentado por los diputados Francisco Jose

Contreras Contreras, Mario Roderico de León Mazariegos y Félix Adolfo Ruano de León, logrando de esta manera proteger la seguridad e intimidad de la población Guatemalteca.

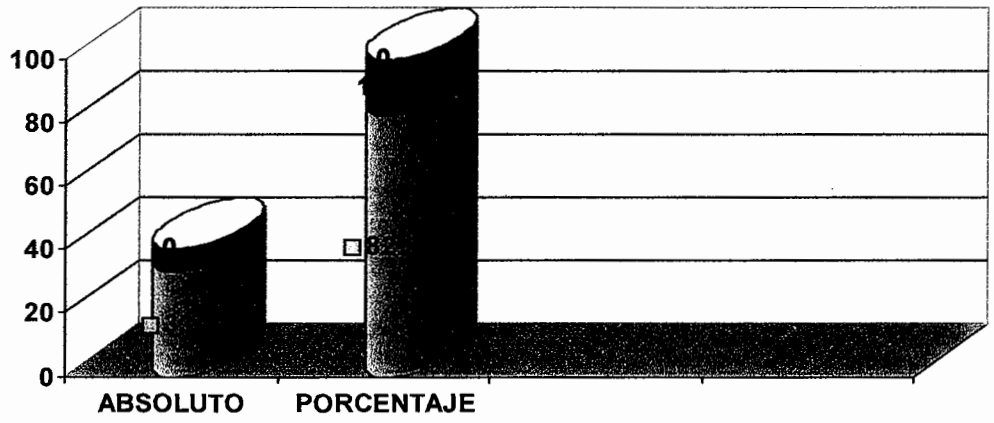
ANEXOS

ANEXO I

Resultado de encuestas a población estudiantil universitaria, campus central Universidad San Carlos de Guatemala, Facultad de Ciencias Jurídicas y Sociales.
Número de entrevistados: 50

1. ¿Considera usted que se violenta el derecho a la seguridad y dignidad de las personas por medio de sistemas de información por red en Guatemala?:

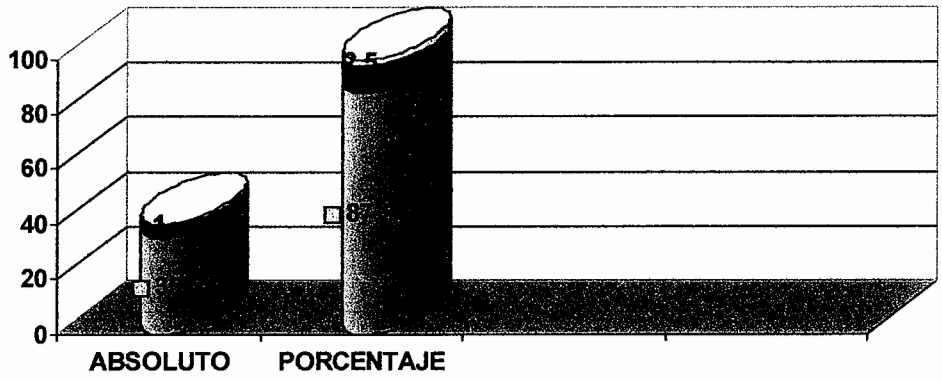
ALTERNATIVA	ABSOLUTO	RELATIVO
SI	48	96%
NO	00	00%
NO CONTESTARON	02	04%
TOTALES	50	100%



INTERPRETACIÓN. Puede establecerse que la mayoría considera que sí se violenta el derecho de la seguridad y dignidad de las personas por medio de la red. Esto fundamenta el temor de la seguridad de sus datos en línea, y a que se vea violentada por el mal manejo de los mismos.

2. ¿Considera usted que existen dificultades en el sistema de justicia de Guatemala para la aplicación de las leyes en todos aquellos actos ilícitos que tengan relación con sistemas de información por red?

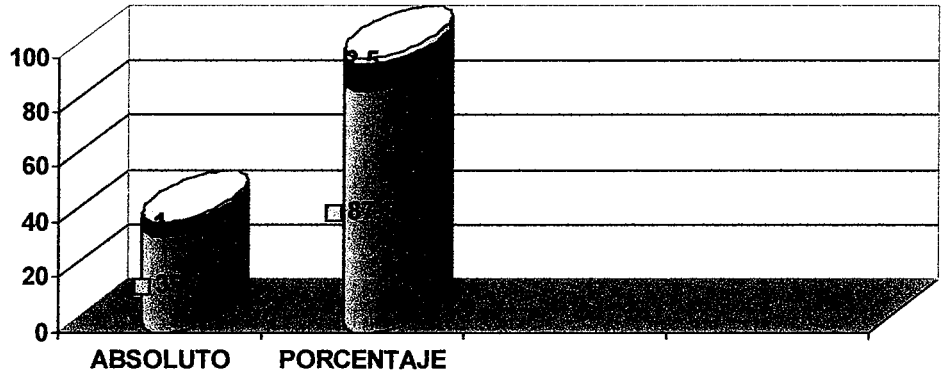
ALTERNATIVA	ABSOLUTO	PORCENTAJE
SI	49	98%
NO	01	02%
NO CONTESTARON	00	00%
TOTALES	50	100%



INTERPRETACIÓN. El 98 % considera que sí existe dificultad por parte del sistema judicial en cuanto a la aplicación de la normativa en los ilícitos informáticos, confirmando así que no existe capacidad por parte del Estado para impartir justicia en cuanto a los delitos cometidos por la red, y para enfrentar a los cibercriminales, por no existir la legislación adecuada a la informática.

3. ¿Considera usted que en el ámbito guatemalteco existen delitos informáticos por robo de información en los sistemas de red y que los mismos afectan la seguridad y dignidad de las personas al ser mal utilizada dicha información?

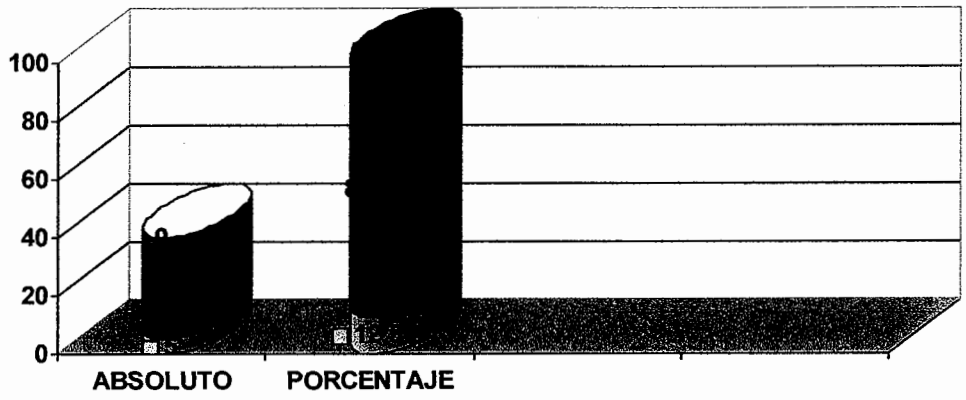
ALTERNATIVA	ABSOLUTO	PORCENTAJE
SI	40	80%
NO	09	18%
NO CONTESTARON	01	02%
TOTALES	50	100%



INTERPRETACIÓN. El 80% indicaron que efectivamente existen delitos informáticos por robo de información en los sistemas de red y que los mismos afectan la seguridad y dignidad de las personas al ser mal utilizada dicha información; pero es importante resaltar como un 18% considera que no existen delitos informáticos que les afecten, o nunca se han visto afectados.

4. ¿Cuál considera usted que puede ser el punto principal en el cual se puede cometer en Guatemala un ciberdelito?

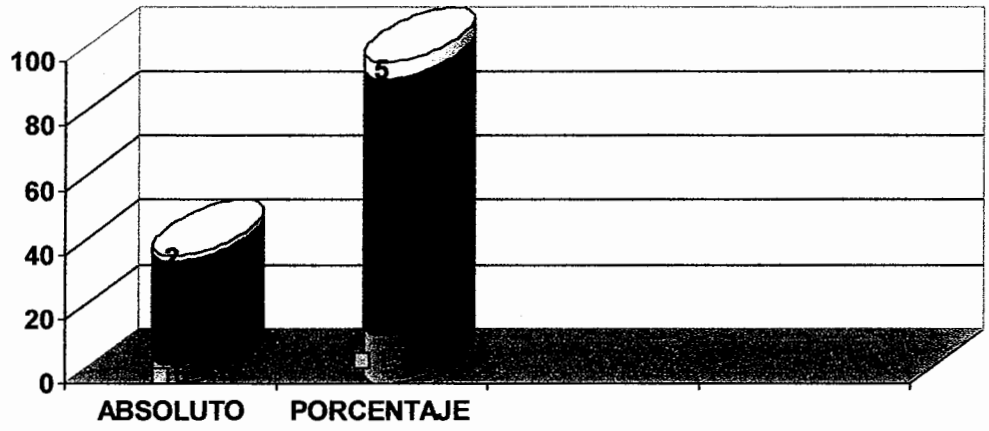
ALTERNATIVA	ABSOLUTO	PORCENTAJE
SISTEMAS INTERNOS	13	26%
CONEXIÓN A INTERNET	37	74%
NO CONTESTARON	00	00%
TOTALES	50	100%



INTERPRETACIÓN. La mayoría considera que los delitos informáticos se realizan a través de la red y la conexión a internet, los delitos informáticos no se limitan a operaciones de circuitos cerrados dentro de instituciones o empresas, va más allá y sobre todo por la globalización de las tecnologías.

5.¿Cuál considera que es el principal abuso o ataque informático que se comete dentro del ámbito guatemalteco en relación a sistemas de información?

ALTERNATIVA	ABSOLUTO	PORCENTAJE
Penetración del sistema del exterior	39	78%
Abusos por parte del empleado	08	16%
Virus de computadora	03	06%
TOTALES	50	100%



INTERPRETACIÓN. El 78% indica que el principal abuso o ataque informático que se comete es la penetración del sistema del exterior; denotando así que la red no es un medio seguro para el manejo de información, pero que si existiese legislación que penara las distintas actividades que violentan la seguridad de la red la población se sentirá más confiada al usar los medios informáticos.

ANEXO II

(No aprobada)

INICIATIVA NÚMERO 4055

EL CONGRESO DE LA REPÚBLICA DE GUATEMALA

CONSIDERANDO:

Que es indispensable la aprobación de una ley especial que contenga disposiciones que tiendan a proteger, integralmente, los sistemas informáticos y bases de datos, a fin de garantizar certeza jurídica en las transacciones propias del comercio electrónico.

CONSIDERANDO:

Que debido a que en nuestro país ya existe regulación sobre comercio electrónico, según el contenido de la Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas, Decreto número 47-2008 del Congreso de la República de Guatemala, se hace necesario emitir una ley especial para prevenir y sancionar los delitos cometidos con ocasión a la normativa de comercio electrónico, y todos aquellos actos ilícitos de naturaleza informática.

CONSIDERANDO:

Que existen normas de carácter internacional que incluyen, dentro de la normativa de Cibercrimen, los actos de pornografía infantil que son difundidos a través de mensajes de datos o sistemas informáticos, lo cual impone la obligación de legislar, a nivel del derecho interno, las normas de prevención y sanción de esos ilícitos.

CONSIDERANDO:

Que es necesaria la efectiva creación y aplicación de normas especiales, toda vez que, por la naturaleza de los actos de cibercrimen, se complica la aplicación de las actuales normas del Código Penal, lo que se traduce en lagunas legales que permiten al delincuente realizar actos ilícitos por medio de las nuevas tecnologías de la información. Así también, se hace necesario crear una unidad especializada para combatir la delincuencia informática.

POR TANTO:

En ejercicio de la atribuciones que le confiere la literal a) del artículo 171 de la Constitución Política de la República de Guatemala.

DECRETA:

La siguiente:

LEY DE DELITOS INFORMÁTICOS

TÍTULO I.

DISPOSICIONES GENERALES

Artículo 1.- Objeto de la ley. Esta ley 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 y demás formas de abuso sexual con menores de edad y que se realicen por medio de sistemas informáticos.

Artículo 2.- Definiciones: Además de las definiciones contenidas en la Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas, Decreto 47-2008 del Congreso de la República, y para los efectos de la presente ley, se entenderá por:

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.

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.

Pornografía infantil: Toda representación de un menor de edad dedicado a actividades explícitas reales o simuladas de carácter sexual, realizada 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, cuanto esta representación no tenga valor artístico, literario, científico o pedagógico.

Sistema informático: Dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, 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.

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

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 información.

Artículo 3.- (Ámbito de aplicación). La presente ley será aplicable a los responsables de los 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 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.

TÍTULO II.

DELITOS CONTRA LA CONFIDENCIALIDAD, LA INTEGRIDAD Y LA DISPONIBILIDAD DE LOS DATOS Y SISTEMAS INFORMÁTICOS

Artículo 4.- (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.

Artículo 5.- (Daño informático). El que ilegítimamente alterare, destruyere, inutilizare, suprimiere, modificare, o de cualquier modo o por cualquier medio, dañare un sistema o dato informático, será penado con prisión de cuatro a ocho años.

Artículo 6.- (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 o preste servicios destinados a cumplir los mismos fines, será penado con prisión de tres a seis años.

Artículo 7.- (Espionaje informático). El que, ilegítimamente, se apodere, 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.

Igual pena se aplicará a quien creare un sistema o datos informáticos que puedan afectar la intimidad o privacidad de las personas.

TÍTULO III.

DELITOS INFORMÁTICOS RELACIONADOS CON LA PROPIEDAD Y AUTENTICIDAD

Artículo 8.- (Fraude informático). El que, para obtener algún beneficio para sí 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.

Artículo 9.- (Uso fraudulento de tarjetas inteligentes o instrumentos análogos). Quien, de manera deliberada e 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.

Artículo 10.- (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 de prisión.

Artículo 11.- (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.

Artículo 12.- (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.

Artículo 13.- (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.

TÍTULO IV.

DELITOS RELACIONADOS CON EL CONTENIDO

Artículo 14.- **(Pornografía infantil)**. 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 de edad, o de una persona que parezca un menor.

Cuando las conductas a 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.

Artículo 15.- (Alteración de imágenes): Quien, de manera deliberada e ilegítima, a través de mensaje de datos o de cualquier otro medio, envíe, transmita o aloje en sistemas informáticos, imágenes o fotografías de personas, con fines exhibicionistas o pornográficos, será sancionado con prisión de tres a seis años y con una multa de diez mil a cien mil quetzales.

Igual pena se aplicará para quien modifique o altere imágenes o fotografías de personas, con fines exhibicionistas o pornográficos, o que menoscaben la dignidad de la persona.

TÍTULO V.

UNIDAD DE INVESTIGACIÓN

Artículo 16.- El Ministerio Público, en un plazo no mayor de sesenta (60) días, creará y organizará una Unidad de Investigación especializada en delitos informáticos a efecto de lograr la debida aplicación de las disposiciones contenidas en la presente ley.

TÍTULO VI.

DISPOSICIONES FINALES

Artículo 17.- (Derogatorias). Se derogan las siguientes normas contenidas en el Código Penal, Decreto 17-73 del Congreso de la República: 274 "A", 274 "B", 274 "C", 274 "D", 274 "E", 274 "F", 274 "G".

Artículo 18.- (Vigencia). La presente ley entrará en vigencia ocho (8) días después de su publicación en el Diario Oficial.

REMÍTASE AL ORGANISMO EJECUTIVO PARA SU SANCIÓN, PROMULGACIÓN Y PUBLICACIÓN.

EMITIDO EN EL PALACIO DEL ORGANISMO LEGISLATIVO, EN LA CIUDAD DE GUATEMALA, MAYO DE DOS MIL NUEVE.

Diputados Ponentes:

Francisco José Contreras Contreras

Mario Roderico de León Mazariegos

Félix Adolfo Ruano de León

BIBLIOGRAFÍA

ALEGRÍA, Ciro. **La seguridad como derecho humano.- El Pensamiento Constitucional.** Lima, Perú: Ed. la Pontificia Universidad Católica del Perú, 2002.

Asociación de Investigación y Estudios Sociales. **Derecho a la seguridad personal. Centro de Documentación** Revista No. 22. Guatemala: Ed. Biblioteca Gonzalo Menéndez de la Riva.1994.

BATTLE, Georgina. **El derecho a la intimidad privada y su regulación**. Alcoy: Ed. Marfil, 1972

CABANELLAS, Guillermo. **Diccionario enciclopédico de derecho usual**. Buenos Aires, Argentina: Ed. Heliasta, S.R.L d., 1989.

COHEN KAREN, Daniel. **Sistemas de información gerencial**. 3ra. Edición. México: Ed. McGraw Hill, 2000.

CRUZ DE PABLO, José Antonio. **Derecho penal y nuevas tecnologías**. Aspectos Sustantivos .Madrid, España: Ed. Grupo Difusión, 2006.

DAVARA RODRÍGUEZ, Miguel Ángel. **Derecho informático.** Pamplona, España: Ed. Aranzadi, 1993.

DAVARA & DAVARA. **Factbook de comercio electrónico**. Pamplona, España: Ed. Aranzadi, 2002.

DESANTES GUANTER, José María. **Hacia una historia del derecho a la información.** Quito, Ecuador: (s.e.), 2006.

FROSINI, VITTORIO. **Cibernética, derecho y sociedad.** Madrid España: Ed. Tecnos, 1982.

Fundación Tomás Moro. **Diccionario Espasa Calpe, S.A.** España: Ed. Norma, 1989.

GARCÍA GONZÁLEZ, Aristeo. **El derecho a la intimidad desde una perspectiva constitucional: equilibrio, alcances, límites y mecanismos de defensa**. México: Ed. Universidad Michoacana de San Nicolás de Hidalgo, Biblioteca de la Facultad de Derecho y Ciencias Sociales, 2005.

http://arbitrajeglobal.com/documents/congr10/10s.pdf **prevención del delito y tratamiento del delincuente** (Guatemala, 23 de enero de 2011)

http://arbitrajeglobal.com/**árticulos delito_informático** (Guatemala, 22 de enero de 2011)

http://www.**deltaasesores**.com (Guatemala, 12 de diciembre de 2010)

http://www.estudding.org/**delito_inform** (Guatemala, 5 de enero de 2011)

http://www.elsalvador.com/**noticias**/2003/05/20/nacional/nacio20.html (Guatemala, 12 de julio 2010)

http://www.**infornet**.com (Guatemala ,17 diciembre de 2010)

http://www.**monografias_sistemasdeinformacion**.com (Guatemala, 12 de diciembre de 2010)

http://www.pieb.org/seguridadciudadana/ **proyecto definición de seguridad** (Guatemala, 15 de diciembre de 2010)

http://www.rae.es/rae.html **definición de seguridad** (Guatemala, 15 de diciembre de 2010)

http://www.**referencia**.infor.net (Guatemala, 20 de enero de 2011)

http://www.uncjin.org/Documents/congr10/10s.pdf **prevención del delito y tratamiento del delincuente** (Guatemala, 23 de enero de 2011)

HUGO VIZCARDO, Silfredo. **Delitos informáticos**. Revista Agora. Facultad de Derecho y Ciencias Políticas - U.I.G.V, Edición Nº 1, Lima Perú: (s.e.), 2004

JENSON, Bárbara. **Acecho cibernético: delito, represión y responsabilidad personal en el mundo online**. (s.l.i.), (s.e.), 1996.

MÉNDEZ VILLASEÑOR, Claudia. **Allanan la sede de infornet**. Guatemala: Ed. Prensa Libre, 2003

MORALES, Sergio. **Informe circunstanciado.** Guatemala: Ed. Procuraduría de los Derechos Humanos, 2003.

MORALES TRUJILLO, Hilda. **Manual de aplicación para la calificación de violaciones a los derechos Humanos.** Guatemala: Ed. Procuraduría de los Derechos Humanos, 2005.

NOGUERA ALCALÁ, Humberto. **Teoría y dogmática de los derechos fundamentales**. México: Ed. Universidad Nacional Autónoma de México, 2003.

O´ BRIEND, James. **Bases de los sistemas de información**. (s.l.i.), Ed. McGraw Hill, 2000.

OSSORIO MELÉNDEZ, A. Hugo. **Políticas de información y derecho. Estudio comparativo.** Chile: Ed. Impresos Universitaria, 1997.

PÉREZ LUÑO, A. **Derechos humanos, estado de derecho y Constitución**, 9a.edición. Madrid, España: Ed. Tecnos, 2005

STUART MILL, John. **Sobre la libertad,** 6a.edición. Madrid España: Ed. Alianza, (s.f.).

TÉLLEZ, Julio. **Derecho informativo, Sistematización y consolidación del derecho, legislación y el manejo de la información en la era del conocimiento.** México: Ed. Granica Reudal, 1996.

Legislación:

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

Declaración Universal de los Derechos Humanos. Asamblea General de las Naciones Unidas, 1948.

Declaración Americana de los Derechos y Deberes del Hombre. Organización de los Estados Americanos, 1948

Convención Americana sobre Derechos Humanos. Organización de los Estados Americanos, 1969.

Convenio de Ciberdelincuencia. Consejo de Europa, 2003.

Código Penal. Congreso de la República de Guatemala, Decreto número 17-94, 1974.

Código Procesal Penal. Congreso de la República de Guatemala, Decreto número 51-92, 1994

Ley de Acceso a la Información Pública. Congreso de la República de Guatemala, Decreto número 57-2008, 2008

Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas. Congreso de la República de Guatemala, Decreto número 47-2008,2008.