

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



**ANÁLISIS DOCTRINARIO DE LOS ELEMENTOS JURÍDICOS QUE DEBE
CONTENER UNA LEGISLACIÓN QUE REGULE EL COMERCIO
ELECTRÓNICO EN GUATEMALA**

BENJAMÍN ANTONIO ESTRADA ZALDAÑA

GUATEMALA, AGOSTO DE 2011

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



**ANÁLISIS DOCTRINARIO DE LOS ELEMENTOS JURÍDICOS QUE DEBE
CONTENER UNA LEGISLACIÓN QUE REGULE EL COMERCIO
ELECTRÓNICO EN GUATEMALA**

BENJAMÍN ANTONIO ESTRADA ZALDAÑA

Guatemala, agosto de 2011

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

**ANÁLISIS DOCTRINARIO DE LOS ELEMENTOS JURÍDICOS QUE DEBE
CONTENER UNA LEGISLACIÓN QUE REGULE EL COMERCIO
ELECTRÓNICO EN GUATEMALA**

TESIS

Presentada a la Honorable Junta Directiva
de la

Facultad de Ciencias Jurídicas y Sociales

de la

Universidad de San Carlos de Guatemala

Por

BENJAMÍN ANTONIO ESTRADA ZALDAÑA

Previo a conferírsele el grado académico de

LICENCIADO EN CIENCIAS JURÍDICAS Y SOCIALES

y los Títulos Profesionales de

ABOGADO Y NOTARIO

Guatemala, agosto de 2011

**HONORABLE JUNTA DIRECTIVA
DE LA
FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES
DE LA
UNIVERSIDAD DE SAN CARLOS DE GUATEMALA**

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

**TRIBUNAL QUE PRACTICÓ
EL EXAMEN TÉCNICO PROFESIONAL**

Primera fase:

PRESIDENTE: Lic. Rodolfo Giovanni Celis López
VOCAL: Lic. Carlos Alberto Velásquez Polanco
SECRETARIO: Lic. Mario Rene Monzón

Segunda fase:

PRESIDENTE: Lic. Héctor Orozco y Orozco
VOCAL: Licda. Eloisa Mazariegos Herrera
SECRETARIO: Lic. Marco Tulio Pacheco Galicia

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).”



Licda. María Haydee Enríquez Sánchez
Abogado y Notario

Guatemala, 28 de abril 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
Ciudad Universitaria



Licenciado Castro Monroy:

De la manera más atenta me permito comunicarle que he cumplido con la función de Asesor de Tesis del bachiller **BENJAMIN ANTONIO ESTRADA ZALDAÑA**, intitulado: **“ANALISIS DOCTRINARIO DE LOS ELEMENTOS JURÍDICOS QUE DEBE CONTENER UNA LEGISLACIÓN QUE REGULE EL COMERCIO ELECTRÓNICO EN GUATEMALA”**; el cual a mi criterio cumple con todos los requisitos y formalidades que establece la normativa de esta facultad, y emito el dictamen siguiente:

- a) El tema investigado por el bachiller **Benjamín Antonio Estrada Zaldaña**, es de suma importancia respecto a su contenido científico y técnico, ya que se presenta con una temática que deviene de explorar el ámbito del Derecho Mercantil, contribuyendo a la importancia de actualizar la ley mercantil, que por la antigüedad se ha convertido en obsoleta y por ende no cumple con su objetivo. Lo técnico se manifiesta en la investigación realizada aportando soluciones siempre respetando el criterio de su autor en la redacción objetiva; además que la investigación realizada, es de carácter jurídico puesto que incorpora mecanismos idóneos a considerar para la solución del problema planteando una alternativa eficaz.
- b) En la investigación realizada, el bachiller empleó los métodos analítico al tener contacto con toda la información bibliográfica de diferentes autores; el método sintético al resumir la información que realmente se consideró importante; el método deductivo al tener contacto con el problema planteado, y posteriormente especificando el tema que ocupaba la presente investigación; el método inductivo durante el desarrollo de la tesis; por lo tanto considero que la estructura de la tesis y, la metodología y técnicas de investigación empleadas, son las adecuadas para el desarrollo del tema y el logro de los objetivos que la investigación pretende arribar.



- d) Con respecto a la contribución científica del trabajo de tesis considero que constituye un aporte científico, válido y oportuno encaminado a solventar sobre los elementos jurídicos que debe de contener una nueva legislación mercantil con respecto al comercio electrónico, a través del aporte que presenta el bachiller ello en virtud que el tópico abordado en dicho trabajo, resulta de singular importancia ya que aborda temas tanto legales como legislativos al indicar que se debe de analizar una modificación en la ley con relación a los recursos administrativos y la necesidad de que los mismos tengan un efecto suspensivo, regulando todos y cada uno de los elementos del mismo.
- e) El bachiller arriba a conclusiones y recomendaciones congruentes con su trabajo, que confirman los supuestos y las hipótesis planteadas al inicio de la investigación, sintetizando y solventando además las afirmaciones que se sustentan en el desarrollo del mismo.
- f) Se evidencia que el bachiller realmente investigó el tema y acudió a las fuentes bibliográficas, tanto doctrinarias como legales, y de campo idóneas para su desarrollo.
- g) En virtud de lo anterior, y por haberse cumplido con los requisitos establecidos en el Artículo 32 del Normativo para la Elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Público, resulta procedente dar el presente **DICTAMEN FAVORABLE, APROBANDO** el trabajo de tesis considerando conveniente la impresión del mismo previo dictamen del señor revisor, para que pueda ser discutido en el correspondiente examen público.

Sin más que agradecer la consideración a mí persona, al encomendarme tan honroso trabajo de Asesor, aprovecho la oportunidad para reiterarle mi alta muestra de estima.

Sin otro particular, me suscribo muy cordialmente.

Licenciada
María Haydée Enríquez Sánchez
ABOGADO Y NOTARIO

Licda. MARÍA HAYDEE ENRÍQUEZ SANCHEZ
Abogado y Notario
Colegiada 3,601
Asesora de Tesis



Guatemala, 28 de septiembre del año 2009.

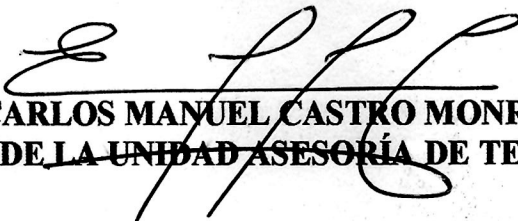
Licenciado (a)
MARÍA HAYDEÉ ENRÍQUEZ SÁNCHEZ
Ciudad de Guatemala

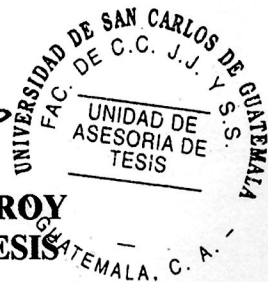
Licenciado (a) Enríquez Sánchez:

Atentamente me dirijo a usted para hacer de su conocimiento que recibí el dictamen del (de la) Consejero (a)- Docente de la Unidad de Asesoría de Tesis de ésta Facultad, en el cual hace constar que el plan de investigación y el tema propuesto por el (la) estudiante: **BENJAMIN ANTONIO ESTRADA ZALDAÑA, CARNE NO.199921055**, intitulado "ANÁLISIS DOCTRINARIO DE LOS ELEMENTOS JURÍDICOS QUE DEBE CONTENER UNA LEGISLACIÓN QUE REGULE EL COMERCIO ELECTRÓNICO EN GUATEMALA" reúne los requisitos contenidos en el Normativo respectivo.

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

"ID Y ENSEÑAD A TODOS"


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



c.c. Unidad de Tesis, interesado y archivo

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA



FACULTAD DE CIENCIAS
JURÍDICAS Y SOCIALES

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



**UNIDAD ASESORIA DE TESIS DE LA FACULTAD DE CIENCIAS
JURÍDICAS Y SOCIALES.** Guatemala, uno de junio de dos mil once.

Atentamente, pase al (a la) LICENCIADO (A): **BYRON OSWALDO CASTAÑEDA GALINDO**, para que proceda a revisar el trabajo de tesis del (de la) estudiante: **BENJAMÍN ANTONIO ESTRADA ZALDAÑA**, Intitulado: **“ANÁLISIS DOCTRINARIO DE LOS ELEMENTOS JURÍDICOS QUE DEBE CONTENER UNA LEGISLACIÓN QUE REGULE EL COMERCIO ELECTRÓNICO EN GUATEMALA”**.

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 ASESORIA DE TESIS



cc.Unidad de Tesis
CMCM/ brsp.



Guatemala, 07 de Junio de 2,011

LICENCIADO
CARLOS MANUEL CASTRO MONROY
JEFE DE LA UNIDAD DE ASESORÍA DE TESIS
FACULTAD DE CIENCIAS JURIDICAS Y SOCIALES
CIUDAD UNIVERSITARIA



Estimado Licenciado Castro Monroy:

Por este medio hago de su conocimiento que de conformidad con lo establecido en el artículo 32 del Normativo para la Elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Público, y de la resolución de fecha 01 de junio del presente año procedí a la revisión del trabajo de tesis del Bachiller BENJAMÍN ANTONIO ESTRADA ZALDAÑA, intitulado: "ANALISIS DOCTRINARIO DE LOS ELEMENTOS JURÍDICOS QUE DEBE CONTENER UNA LEGISLACIÓN QUE REGULE EL COMERCIO ELECTRÓNICO EN GUATEMALA".

En relación a los métodos utilizados en la elaboración del Trabajo de investigación realizado por el Bachiller BENJAMIN ANTONIO ESTRADA ZALDAÑA, fue implementada una temática adecuada, empleando métodos analíticos inductivos y deductivos y una bibliografía atinada, realizado de conformidad con los métodos modernos para la investigación y elaboración de un trabajo de tesis.

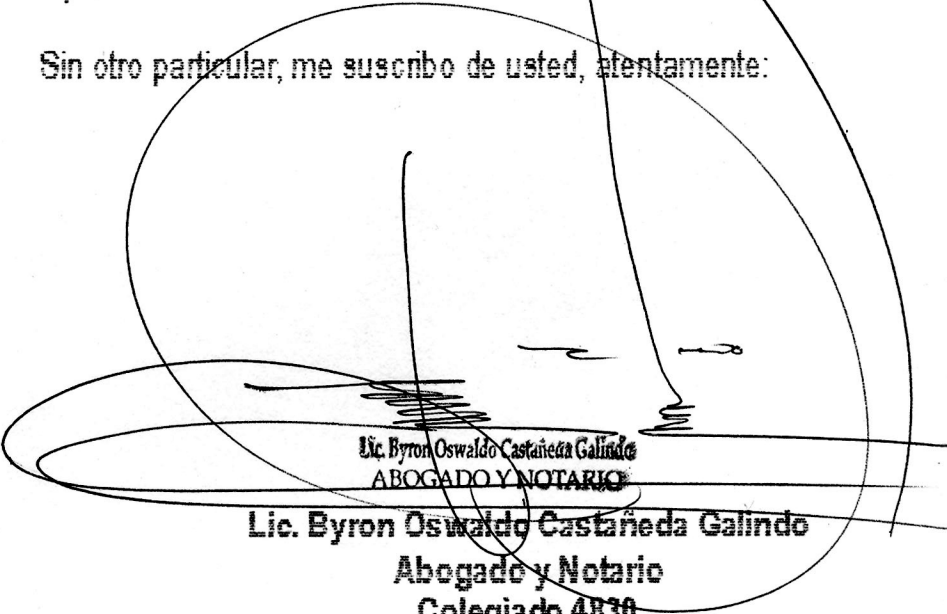
Con relación al tema elegido por el Bachiller BENJAMIN ANTONIO ESTADA ZALDAÑA, intitulado "ANALISIS DOCTRINARIO DE LOS ELEMENTOS JURÍDICOS QUE DEBE CONTENER UNA LEGISLACIÓN QUE REGULE EL COMERCIO ELECTRÓNICO EN GUATEMALA". Es un tema de actualidad, puesto que las variantes dentro del Derecho Mercantil internacional se basa en gran parte al comercio electrónico, lo cual no es ajeno al sistema guatemalteco, por lo que las propuestas efectuadas de una legislación relacionada al tema, conteniendo los elementos jurídicos adecuados, es de suma importancia y de invalorable aporte a nuestro ordenamiento. La redacción que se empleó en el presente trabajo de tesis es el adecuado.



Las conclusiones y recomendaciones realizadas en el trabajo de tesis objeto de revisión son congruentes y nuevamente constituyen un aporte de suma valía para el campo del comercio electrónico en Guatemala.

En virtud de lo antes expresado, y por cumplir a cabalidad a mi criterio con los requisitos legales citados anteriormente, es procedente emitir DICTAMEN FAVORABLE al trabajo de tesis "ANÁLISIS DOCTRINARIO DE LOS ELEMENTOS JURÍDICOS QUE DEBE CONTENER UNA LEGISLACIÓN QUE REGULE EL COMERCIO ELECTRÓNICO EN GUATEMALA", aprobando el mismo, y sugiriendo a las Autoridades de la Facultad de Ciencias Jurídicas y Sociales de la Universidad de San Carlos de Guatemala que el mismo pueda ser defendido por el ponente en el examen público de tesis.

Sin otro particular, me suscribo de usted, atentamente:



Lic. Byron Oswaldo Castañeda Galindo
ABOGADO Y NOTARIO

Lic. Byron Oswaldo Castañeda Galindo
Abogado y Notario
Colegiado 4830
Revisor de Tesis

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA



FACULTAD DE CIENCIAS
JURÍDICAS Y SOCIALES

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

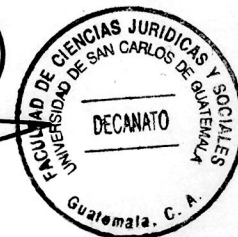


DECANATO DE LA FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES.

Guatemala, siete de julio del año dos mil once.

Con vista en los dictámenes que anteceden, se autoriza la Impresión del trabajo de Tesis del (de la) estudiante BENJAMIN ANTONIO ESTRADA ZALDAÑA, Titulado ANÁLISIS DOCTRINARIO DE LOS ELEMENTOS JURÍDICOS QUE DEBE CONTENER UNA LEGISLACIÓN QUE REGULE EL COMERCIO ELECTRÓNICO EN GUATEMALA. 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



DEDICATORIA

- A DIOS:** Por haberme dado la vida y mostrado el camino.
- A MIS PADRES:** Benjamín Estrada Barrera y Dora Judith Zaldaña García de Estrada, como un ejemplo, por sus múltiples sacrificios y desvelos.
- A MIS HERMANOS:** Erick Estuardo, Carol Judith, y Sergio Alejandro. Por su ayuda incondicional y por haber compartido tristezas y alegrías en nuestro caminar y creer siempre en que lograría culminar mi carrera.
- A MI HIJA:** Natalia Estrada por ser mi inspiración, mi luz y mi vida.
- A MIS AMIGOS:** En especial a Violeta, Esbin y todas aquellas personas que me brindaron ayuda y amistad.
- A MI GUATEMALA:** Con amor patrio, orgulloso de haber nacido en esta tierra bendita de Dios.
- A:** La Gloriosa y Tricentenaria Universidad de San Carlos de Guatemala, en especial a la Facultad de Ciencias Jurídicas y Sociales.

ÍNDICE

	Pág.
Introducción.....	i

CAPÍTULO I

1. Derecho informático.....	1
1.1. Derecho Informático.....	04
1.2. Tendencia internacionales de la información y el derecho	08

CAPÍTULO II

2. La evolución de internet.....	11
2.1. Antecedentes de internet.....	14
2.2. Servicios de internet.....	19
2.3. Principales problemas de internet.....	21
2.4. Derecho a la intimidad.....	24
2.5. Regulación internacional de Internet.....	27

CAPÍTULO III

3. Comercio electrónico.....	35
3.1. Medios electrónicos de pago.....	36
3.2. Las características generales de los contratos a través de Internet. Una nueva forma de concebir la contratación.....	41
3.3. Puntos débiles de las transacciones electrónicas.....	43
3.4. El contrato marco.....	49

CAPÍTULO IV

4.	Los fundamentos doctrinarios que definen la creación de una norma que regule el comercio electrónico en Guatemala.....	55
4.1.	La protección jurídica en Internet.....	56
4.2.	La situación legal de Internet en Guatemala.....	58
4.3.	Los fundamentos jurídicos que informan a una norma sobre comercio electrónico en Guatemala.....	61
	CONCLUSIONES.....	85
	RECOMENDACIONES.....	87
	BIBLIOGRAFÍA.....	89

CAPÍTULO I

1. Derecho informático

En los albores de la sociedad del conocimiento, se ha originado una revolución industrial, relativa a las nuevas tecnologías que conlleva un nuevo avance de la humanidad donde el compartir los conocimientos a través de la información es el objetivo principal.

En este apartado se hará referencia específicamente a la relación entre el derecho y la informática que es la base o fuente fundamental de la sistematización del derecho, que no es más que el ordenamiento, análisis y utilización de la tecnología informática encaminada a la evolución del derecho en todas sus áreas y la utilización del mismo para el desarrollo de las sociedades y la consolidación de un Estado democrático.

a) Relación entre derecho e informática: La relación entre derecho e informática se manifiesta de dos maneras:

- Los aspectos normativos del uso de la informática, desarrollados bajo el derecho de la Informática.

- La aplicación de la informática en el tratamiento de la información jurídica.

Para el desarrollo de la informática jurídica es necesario considerar ciertos elementos de origen, como son:

- La aplicación de la lógica del derecho o raciocinio jurídico.

- Análisis del discurso jurídico o sistema normativo.
- Aplicación de la teoría de los sistemas.
- Aplicación de la teoría de la información.

Todos estos elementos constituyen la base fundamental para complementar el objeto mismo de la informática jurídica.

El desarrollo de la informática jurídica tiene como principal función el ordenamiento y el análisis del discurso jurídico y su fin es la creación de instrumentos que permitan el acceso a la información jurídica.

b) Definiciones y clasificación de la informática jurídica: “La informática jurídica es la técnica interdisciplinaria que tiene por objeto el estudio e investigación de los conocimientos de la informática general, aplicables a la recuperación de información jurídica, así como la elaboración y aprovechamiento de los instrumentos de análisis y tratamiento de información jurídica necesarios para lograr dicha recuperación, es decir como instrumento puesto al servicio de la ciencia jurídica”.¹

La informática jurídica vista como una forma de análisis u ordenación de la información está dividida en:

- a) Informática jurídica
- b) Informática jurídica de gestión, de administración o control, ofimática.

¹ Losano, Mario G. **Curso de informática jurídica**. Pág. 21

c) Informática jurídica meta decisional o meta documental o de ayuda a la decisión

La informática jurídica, se desprende del análisis de la información contenida en documentos jurídicos para la formación de datos documentales.

Es la aplicación de la informática jurídica en los aspectos sobre el análisis, archivo y recuperación de información contenida en la legislación, jurisprudencia, doctrina o cualquier otro documento con contenido jurídico relevante.

Para manifestar de informática jurídica, se necesita identificar la información, que en este caso será la jurídica, toda aquella pertinente al caso concreto; es determinante tratarla por medio de la estructuración con la aplicación de la lógica o la argumentación para, posteriormente, mediante los instrumentos lingüísticos apropiados, incorporarla a la computadora.

No será informática jurídica documental la simple incorporación de textos jurídicos a una computadora.

Mientras que a la informática jurídica de gestión, administración o control se le denomina ofimática, la cual organiza y controla la información jurídica de documentos, expedientes, libros, mediante la aplicación de programas de administración que permitan crear identificadores y descriptores para la clasificación de dicha información,

la cual es utilizada en tribunales, despachos, notarías, oficinas jurídicas, para seguimiento de trámites y procesos.

Por aparte, la informática jurídica de meta decisional, meta documental o de ayuda a la decisión se conforma por bases de conocimiento jurídico, que incluye sistemas expertos legales que permite emitir conclusiones a partir de la información que se le suministra en forma de pregunta y respuesta, siendo la misma una base de datos con información confiable, lo cual la hace un sistema de enseñanza del derecho asistido por computadoras.

1.3. Derecho informático

El binomio Informática y derecho, indica con claridad la interacción entre dos ciencias de la cual surge un campo fecundo del saber, por una parte la computadora se considera un instrumento utilizado por el jurista para crear bancos de datos jurídicos y por otra recurrir a la computadora plantea una serie de problemas que deben ser regulados por la ley.

Especificando, se puede conceptualizar como: “El conjunto de normas jurídicas que regulan la creación, desarrollo, uso aplicación de la informática o los problemas que es o debe de ser tutelado jurídicamente por las propias normas”.²

² Téllez, Julio. **Derecho informático**. Pág. 17

El derecho informático, “es el conjunto de normas que regulan acciones, procesos, productos y relaciones jurídicas surgidas en torno a la informática y sus aplicaciones.”³

Los campos en los que se aplica la informática que se relacionan con el campo del derecho son los siguientes:

- La Protección jurídica de la información personal que incluye datos particulares o personales que se almacenan o respaldan en soportes automáticos de información, ejemplo: credenciales de identificación oficial ciudadana, cédulas, credenciales electorales.
- Apertura de cuentas bancarias, donde se aportan datos que están íntimamente ligados al derecho a la intimidad, a la vida, a la integridad física, la libertad, y el honor.

La efectiva protección de la intimidad en la sociedad moderna dependerá no solamente de la protección de la protección jurídica de la esfera de la libertad personal, sino también de la regulación del manejo de la circulación de los datos personales informatizados que de los ciudadanos se haga.

Los legisladores europeos fueron los primeros en considerar los efectos socio-jurídicos provocados por la informatización en la sociedad. La consagración constitucional de este derecho como una garantía individual es un deber de todo Estado contemplarlo.

³ **Ibíd.**

“Algunos países como Francia, Dinamarca, España, tienen destinada la tutela y vigilancia de sus disposiciones normativas sobre el manejo, uso y difusión de la información personal a autoridades administrativas, con funciones inspectoras, sancionadoras y de información a los interesados. En Colombia, Brasil, Perú, aparece el llamado Habeas Data, como una nueva instancia procesal destinada a la defensa del ciudadano frente al abuso de poder informático en los registros o bancos de datos de entidades públicas o privadas”.⁴

De esta manera, el Habeas Data, figura destinada a proteger la libertad informática opera en rigor como una modalidad de amparo aunque con finalidades específicas.

a) La protección jurídica de programas para ordenador o software: La protección de la propiedad intelectual en el mercado mundial ha tomado creciente significación en los recientes años y existe una presión fuerte por parte de los propietarios de tecnología del mundo desarrollado para obtener un régimen legal que respalde la autoría, exigen incorporar a la protección jurídica estos programas de cómputos en el ámbito del derecho y de armonización de reglamentaciones.

Así mismo al “respecto a los aspectos esenciales del derecho de la propiedad intelectual en derechos autorales en materia de cómputos, pero sobre todo, en los problemas de derecho de autor de la distribución electrónica de documentos, de la Comunidad Europea y la Organización Mundial de la Propiedad Intelectual (OMPI) señalan que deben circunscribirse en:

⁴ Su, Emilio. **Introducción a la informática jurídica y al derecho de la información.** Pág. 14

- Un nuevo derecho que se aplicará a todas las bases de datos publicadas que envuelvan inversiones de talento y dinero, no solamente a las bases de datos que sean por si misma creaciones intelectuales originales.
- El nuevo derecho se aplicará a todas las bases de datos publicadas, esté o no su contenido protegido bajo derechos de autor.
- El nuevo derecho tendrá una adecuada duración (50 años de la primera aplicación, renovables en razón de cambios sustanciales en el contenido.
- El nuevo derecho no estará sujeto a excepciones que lo transformen en inaplicable.
- El nuevo Derecho se aplicará tanto a los usuarios comerciales como no comerciables”.⁵

La transmisión de datos a través de las fronteras da origen a una nueva problemática jurídica con repercusiones en el derecho público y privado, porque la convergencia de la Informática y las telecomunicaciones, denominada telemática, aumenta la facilidad con que puedan entrar y salir los datos de un país, sin posibilidad efectiva de controlarlos a partir que las fronteras físicas se diluyen así bajo el avance tecnológico y ponen en entre dicho el ejercicio de la soberanía política de los Estados, debiendo establecer sus normas jurídicas locales porque a través de ellas se protegerá el interés internacional y viceversa.

⁵ **Ibíd.** Pág. 15

b) Los delitos informáticos: La teoría del delito aduce que el delito es la conducta típica, antijurídica y culpable a la que se asocia como consecuencia una pena.

Mientras los delitos informáticos no se encuentran tipificados, estos no existen, por tal razón los Estados se deben de preocupar por legislar en la materia.

La Organización para la Cooperación Económica y el Desarrollo –OCDE- establece que: “Cometerá delito informático la persona que maliciosamente use o entre a una base de datos, sistema de computadoras o red de computadoras o a cualquier parte de la misma con el propósito de diseñar, ejecutar o alterar un esquema o artificio, con el fin de defraudar, obtener dinero, bienes o información. También comete este tipo de delito el que maliciosamente y a sabiendas y sin autorización intercepta, interfiere, recibe, usa, altera, daña o destruye una computadora, un sistema o red de computadoras o los datos contenidos en la misma, en la base, sistema o red”.⁶

1.4. Tendencias internacionales de la informática y el derecho

En las tendencias internacionales de la informática y el derecho, se encuentra que existen cuatro niveles de agrupamiento de acuerdo al grado de desarrollo del derecho informático:

“a. Tendencia inicial o básica

b. Tendencia creciente o progresiva

⁶ Guerrero, María Fernanda. **La inteligencia artificial aplicada al derecho**. Pág. 25.

c. Tendencia avanzada o próspera

d. Tendencia culminante o innovadora”.⁷

La primera de estas se caracteriza por el poco avance y desarrollo de la informática jurídica y del derecho informático, debido a la escasa importancia dada a la materia por los funcionarios de gobierno, encontrándose la doctrina sobre esta rama del saber jurídico en un desarrollo inicial.

La tendencia creciente o progresiva se caracteriza porque existe una clara distinción entre informática jurídica y derecho informático, como ramas totalmente independientes, pero relacionadas entre sí, por lo que se considera al derecho informático como rama autónoma del derecho. En Europa se recomienda aglutinar a ambas materias bajo la denominación de informática y derecho por considerar más completa esta definición.

En tercer lugar se encuentra la tendencia avanzada o próspera que destaca la necesidad e importancia de desarrollar la labor legislativa al respecto al derecho informático, normas específicas que regule su aplicación; auge importante respecto a la doctrina y jurisprudencia, por ejemplo delitos informáticos.

Por último la tendencia culminante o innovadora se caracteriza por avances importantes respecto de la informática jurídica metadocumental, así como centros de investigación para utilizar sistemas de inteligencia artificial aplicados al derecho.

⁷ **Ibíd.** Pág. 27

La informática jurídica y el derecho informático, tras denodados esfuerzos por consolidarse como ramas autónomas del Derecho, constituyen dos de las más recientes áreas del derecho que implican un punto de contacto, un lugar de encuentro, entre el derecho y las nuevas tecnologías; en ese sentido, la informática jurídica y el derecho informático hasta cierto punto constituyen las áreas de avanzada del derecho.

No obstante lo anterior, no es tanta la novedad que hasta ahora pueden exhibir estas nuevas disciplinas jurídicas, como inicialmente pudiera parecer; ya que, comparados con los enormes efectos renovadores que tienen las nuevas tecnologías en la economía, en la sociedad y en la cultura en general, el impacto en el derecho es menor; debido a que la esencia del fenómeno tecnológico se haya disminuido, cuando no, mal entendido en su asimilación por el derecho, al hacerse uso en su recepción, de una perspectiva demasiado tradicional del derecho, que además de ser insuficiente para entenderla y regularla, le es incongruente.

CAPÍTULO II

2. La evolución de Internet

Internet es una gran red de redes que recorre prácticamente todo el planeta y hace posible que usuarios de todo el mundo se conecten. Pero ésta es una definición conceptual, ya que internet realmente es algo más.

Es sobre todo y ante todo un gran universo de comunicación, un nuevo mundo virtual en el que prácticamente se puede encontrar cualquier cosa que se deseé buscar, porque en el presente es el único canal de comunicación y expresión realmente libre que existe en el mundo, puesto que se puede entrar a debatir cualquier tema, expresar opinión sobre cualquier cosa, siendo un medio de expresión único, a la vez que universal, para que todas las personas puedan verter en él sus inquietudes, sus trabajos o sus obras.

La forma más habitual y económica de conectarse a esta red de comunicación internacional, consiste en contratar el acceso con una de las numerosas empresas que ofrecen el servicio de conexión. Estas empresas se conocen con el nombre de proveedores de acceso a internet. Para conectarse a internet es necesario cuatro cosas:

- Tener un ordenador.
- Disponer de los programas necesarios, o simplemente tener instalado Windows 95.

-Un módem, o disponer de una red local con salida a internet.

-Una cuenta en internet.

Los proveedores disponen de varios ordenadores lo suficientemente potentes como para asegurar el acceso a varios usuarios. También cuentan con líneas de acceso a internet lo suficientemente anchas y veloces como para asegurar el acceso a todos ellos. Contratar este tipo de líneas supone un coste muy elevado por lo que resultaría muy caro para un usuario normal. Estas empresas revenden el acceso a cada usuario, cuando éstos lo solicitan.

“El internet, es un espacio único donde se intercambia una gran cantidad de contenidos, muchos de ellos considerados lícitos o ilícitos según la legislación internacional y las legislaciones nacionales correspondientes, dicha red ya no es únicamente utilizada con fines académicos, empresariales o militares, sino dado su proceso de expansión se ha abierto a toda la sociedad lo cual lo ha dotado de una dinámica sin precedente.

Hasta el momento Internet solo se ha sujetado a la autorregulación y al trabajo que diversas organizaciones no gubernamentales han realizado para crear un ambiente adecuado para el uso de Internet, principalmente en aspectos técnicos, visuales e incluso comerciales”.⁸

⁸ Siyan, Karanjit. **Internet y seguridad en redes**. Pág. 16

Así mismo, el internet, es a la vez una oportunidad de difusión mundial, un mecanismo de propagación de la información y un medio de colaboración e interacción entre los individuos y sus ordenadores independientemente de su localización geográfica, debido a que resulta siendo una enorme red de comunicaciones de ámbito mundial que permite la interconexión de sistemas informáticos, independientemente de su tipo y situación.

Está físicamente compuesta por ordenadores de diversos tipos, marca y sistema operativo y ruteador que están distribuidos por todo el mundo y unidos a través de enlaces de comunicaciones muy diversos. Sobre estos ordenadores, y aprovechando los servicios de comunicaciones de la red, se ejecutan diversos tipos de aplicaciones, que permiten realizar intercambios muy sofisticados de información.

“Al definir a internet como una ‘red de redes’, es decir, una red que no sólo interconecta computadoras, sino que interconecta redes de computadoras entre sí. Una red de computadoras es un conjunto de máquinas que se comunican a través de algún medio (cable coaxial, fibra óptica, radiofrecuencia, líneas telefónicas, etc.) con el objeto de compartir recursos. De esta manera, el internet sirve de enlace entre redes más pequeñas y permite ampliar su cobertura al hacerlas parte de una red global. Esta red global tiene la característica de que utiliza un lenguaje común que garantiza la intercomunicación de los diferentes participantes; este lenguaje común o protocolo (un protocolo es el lenguaje que utilizan las computadoras al compartir recursos) se conoce como TCP/IP”.⁹

⁹ **Ibíd.**

Este sistema de comunicación global funciona básicamente como el centro de documentación más grande y completo del mundo, pues permite el acceso a libre información sin límites geográficos, fronteras ni jurisdicción y como medio de comunicación a través del correo electrónico, foros de discusión y servicio de llamadas telefónicas.

2.1. Antecedentes de internet

“El cuatro de Octubre de 1957, la antigua Unión de Repúblicas Socialistas Soviéticas puso en órbita el primer satélite artificial, llamado Sputnik, adelantándose a los Estados Unidos de América, que dos años antes había anunciado el inicio de una carrera interestelar. Este importante hecho marca el comienzo del uso de las comunicaciones globales. Un año después el presidente Dwight Eisenhower, ordenó la creación de la Advanced Research Projects Agency (ARPA) creado por el Departamento de Defensa de los EUA, así como la Agencia Nacional de Aeronáutica y del Espacio (NASA, por sus siglas en inglés)”.¹⁰

La primera descripción documentada del” proyecto ARPA está contenida en una serie de memorándums escritos por J.C.R. Licklider, en Agosto de 1962, en los cuales expone su concepto de red galáctica. El concibió una red interconectada globalmente a

¹⁰ **Ibíd.** Pág. 21.

través de la que cada uno pudiera acceder desde cualquier lugar a la información y los programas. En esencia, el concepto era muy parecido al Internet actual.”¹¹

Entre los años de 1962 y 1968 se trabajó el concepto de intercambio de paquetes informativos de origen y uso meramente militar. La idea consistía en que varios grupos de datos pudiesen tomar diferentes rutas para uno o más determinados destinos, consiguiendo con ello una mejor seguridad en su transporte.

En el transcurso del tiempo se siguieron conectando computadores rápidamente a “la ARPANET durante los años siguientes y el trabajo continuó para completar un protocolo host a host funcionalmente completo, así como software adicional de red. En Diciembre de 1970, el Network Working Group (NWG) acabó el protocolo host a host inicial para ARPANET, llamado Network Control Protocol (NCP). Cuando en los nodos de ARPANET se completó la implementación del NCP durante el periodo 1971-72, los usuarios de la red pudieron finalmente comenzar a desarrollar aplicaciones. En Septiembre de 1972, Ray Tomlinson, de BBN (Bolt, Beranek and Newman), escribió el software SENDMSG, de envío-recepción de mensajes de correo electrónico, impulsado por la necesidad que tenían los desarrolladores de ARPANET de un mecanismo sencillo de coordinación”.¹²

¹¹ **Ibíd.**

¹² Jijena Leiva, Renato. **El derecho y la sociedad de la información: la importancia de Internet en el mundo actual.** Pág. 89

En Octubre de 1972, se organizó una gran y muy exitosa demostración de las redes informáticas en la conferencia internacional de comunicaciones computacionales. Esta fue la primera demostración pública de la nueva tecnología de red. Fue también en el año de 1972 cuando se introdujo la primera aplicación del correo electrónico.

Se expandió el valor de este moderno sistema de comunicación, porque surge el primer programa de utilidad de correo electrónico para relacionar, leer selectivamente, almacenar, reenviar y responder a mensajes. Desde entonces, su aplicación se convirtió en la mayor de la red durante más de una década. Fue precursora del tipo de actividad que se observa hoy día en la red, es decir, del enorme crecimiento de todas las formas de tráfico persona a persona.

“A fines de 1972 el ARPANET fue renombrado como DARPANET (The Defense Advanced Research Projects Agency). En 1973 se empezó el desarrollo del protocolo que más tarde se llamaría TCP/IP desarrollado por Vinton Cerf de la Universidad de Standford. El Dr. Robert M. Metcalfe desarrolla en 1976 ‘Ethernet’ cuyo sistema permite el uso de cables coaxiales que permiten transportan la información en forma más rápida. DARPANET empieza a usar el protocolo TCP/IP. Ese mismo año se crea en los Laboratorios de la Bell de AT&T el UUCP (Unix to Unix Copy) distribuido con UNIX un año más tarde. Posteriormente se crea USENET, una red para intercambio de noticias grupales, y que fuera creado por Steven Bellovin y los programadores Tom Truscott y

Jim Ellis, bajo la tecnología de UUCP. Al mismo tiempo IBM crea BITNET (Because it is Time Network) que sirve para mensajes de correo y listas de interés”.¹³

La fundación nacional para la ciencia crea en el año de 1981 una red de comunicaciones llamada CSNET que transmite a 56 kbps, sin necesidad de acceder a ARPANET y es en este año que se empieza a independizar el control científico civil del control militar. En el año de 1983 se crea el Internet Activities Board. Para Enero de ese año todos los equipos conectados a ARPANET tenían que usar el protocolo TCP/IP que reemplazó al NCP, por completo. Para el año de 1984 la ARPANET se dividió en dos redes centrales: MILNET Y ARPANET. La primera era de uso estrictamente militar y la segunda servía para mantener la investigación científica.⁹ Sin embargo el Departamento de Defensa de los EUA seguía controlando ambas.

“En los siguientes dos años la National Science Foundation (NSF) conectó seis centros de súper computación a través del país. Esta red es llamada la NSFNET, o sea la troncal (backbone) de la NSF. Para expandir el acceso a Internet, la NSF auspició el desarrollo de redes regionales, las cuales fueron conectadas al troncal de la NSFNET. Sumándolo a esto la NSF apoyó a instituciones, tales como universidades y centros de investigación, en sus esfuerzos para conectarse a las redes regionales. La NSF otorgó una concesión a Merit Network, Inc. en 1987 para operar y administrar futuros desarrollos de la troncal de la NSFNET. Merit Network Inc. en una asociación con IBM,

¹³ **Ibíd.**

Corp. y con MCI Telecommunications, emprendieron investigaciones para el rápido desarrollo de nuevas tecnologías para redes”.¹⁴

En el año de 1989 la plataforma de la red es mejorada, con ello la red queda habilitada para transmitir datos de hasta uno punto cinco millones de bits por segundo, o lo que es lo mismo hasta 50 páginas de texto por segundo.

La ARPANET es disuelta definitivamente en el año de 1990. Sin embargo un año después la Universidad de Minnesota crea Gopher, una herramienta que facilita enormemente el uso de la Internet, provee al usuario de un método basado en un menú jerárquico, que es capaz de localizar información.

“En 1992 se funda la Internet Society y al año, el European Laboratory for Particle Physics in Switzerland (CERN) libera el World Wide Web (www), desarrollado por Tim Berners-Lee. El www usa el protocolo de transferencia de hipertexto (http) y encadena hipertextos muy fácilmente, cambiando así la ruta o camino de la información, la cual entonces puede ser organizada, presentada y accedida en la Internet. La troncal de la red NSFNET es elevada a ‘T3’ lo que lo habilita para transmitir datos a una velocidad de 45 millones de bits por segundo, o sea cerca de 1400 paginas de texto por segundo”.¹⁵

Posteriormente aparecen el visualizador (browsers) gráfico de Web Mosaic y Netscape Navigator y rápidamente son difundidos por la comunidad de la Internet.

¹⁴ **Ibíd.**

¹⁵ Krol, Ed. **Conéctate al mundo de internet.** Pág. 23

“Debido a su naturaleza intuitiva y a la interfaz gráfica, estos browsers hacen que los www y la Internet sean más atractivos al público en general. Para 1995 la troncal de la red NSFNET es reemplazado por una nueva arquitectura de redes, llamada VBNS (very high speed backbone network system), esto significa sistema de redes con troncal de alta velocidad, que utiliza los Network Service Providers, (proveedores de servicios de redes), redes regionales y Network Access Points (NAPs)”.¹⁶

El 24 de octubre de 1995, el Consejo Federal de la Red aceptó unánimemente una resolución definiendo el término de Internet. Su significado fue elaborado por personas de las áreas de redes y derechos de propiedad intelectual. El concepto hace referencia a un sistema global de información que está relacionado lógicamente por un único espacio de direcciones global basado en el protocolo de Internet (IP) o en sus extensiones, que emplea, provee, o hace accesible, privada o públicamente, servicios de alto nivel en capas de comunicaciones y otras infraestructuras. Actualmente hay más de tres millones de sitios registrados con más de 40 millones de usuarios.

2.2. Servicios de internet

Las posibilidades que ofrece internet se denominan servicios. Cada servicio es una manera de obtener provecho a la red independiente de las demás. Hoy en día, los servicios más usados en Internet son: Correo Electrónico, World Wide Web, FTP, Grupos de Noticias, IRC y Servicios de Telefonía.

¹⁶ **Ibíd.**

El correo electrónico, permite enviar cartas escritas con el ordenador a otras personas que tengan acceso a la Red; el mismo es casi instantáneo, a diferencia del correo normal, y además muy barato; este mecanismo es muy utilizado en el área laboral, pues su uso trae consigo un considerable ahorro de llamadas; asimismo, tiene un gran potencial en el intercambio de información, ya que reduce de modo importante el tiempo de transferencia.

“La World Wide Web, o www, como se suele abreviar, se inventó a finales de los ´80 en el CERN, el Laboratorio de física de partículas más importante del mundo. Se trata de un sistema de distribución de información tipo revista. En la red quedan almacenadas lo que se llaman páginas web, que no son más que páginas de texto con gráficos o fotos. Este sistema de visualización de la información revolucionó el desarrollo de internet, y en ellas se puede tener acceso a información de todo tipo. Muchas empresas están entrando al mercado de internet, especialmente las de prestación de servicios como: agencias de viaje, agentes financieros o de bienes raíces, que necesitan proporcionar a sus clientes información dinámica y actualizada. Los servicios de telefonía son las últimas aplicaciones que han aparecido para internet. Permite establecer una conexión con voz entre dos personas conectadas a internet desde cualquier parte del mundo sin tener que pagar el coste de una llamada internacional. Algunos de estos servicios incorporan no sólo voz, sino también imagen. A esto se le llama videoconferencia”.¹⁷

¹⁷ Montesinos Gutiérrez, Antonio. **La sociedad de la información e internet**. Pág. 24

2.3. Principales problemas de internet

La red fue pensada para que la información fluya libre, ese es su espíritu original. El internet hace posible tanto la difusión genérica de información como su distribución a destinatarios específicos, lo que incrementa su importancia comercial pero genera riesgos adicionales de responsabilidad civil, por el contenido de la información. El conflicto se da entre la ausencia de regulación de contenidos de imágenes, de audio o de textos, o bien la restricción de acceso a través de los poderes públicos o de órganos de control autorizados con respecto a determinados contenidos digitales, en forma análoga a lo que sucede con la difusión audiovisual.

La información disponible en la red puede clasificarse según su contenido en ilícitos y nocivos. Los contenidos ilegales permiten una delimitación más ajustada, por la sanción penal que envuelven dichas conductas en cada país, en las que existe cierto consenso internacional entre las cuales destacan la apología al terrorismo, la pornografía infantil, la provocación o incitación al odio de una raza, etnia o grupo, la difamación en línea claramente maliciosa y la distribución de material soez que viola la dignidad humana, más otras conductas que sólo envuelven una infracción civil como sería la violación de la intimidad de los datos personales o la vulneración de los derechos de autor.

Mientras que los contenidos nocivos se configuran alrededor de una línea divisoria más subjetiva porque se manifiestan a través del juicio de valor que provocan en su destinatario por su nacionalidad, por su religión o por sus concepciones políticas,

raciales o morales efectos negativos, las cuales ciertamente varían de una cultura a otra con mayor facilidad y pueden o no merecer reproche penal, aspecto que hace más difícil su persecución.

En ambos casos, se parte de la base que existe una restricción esencial de carácter ético en su difusión por parte del responsable de su emisión. Del mismo modo, se debe partir de la premisa que en el marco liberal que informa el ordenamiento legal guatemalteco, ningún sistema de filtrado o de bloqueo es capaz de sustituir a la utilización instruida y éticamente responsable de este medio por parte del usuario final, o al control del mensaje indecente a través del paradigmático buen padre de familia cuando es operado por menores de edad.

La noción de contenido de lo ilícito y lo nocivo en Internet en ningún caso es uniforme, ya que ésta se refiere esencialmente a información y, por lo tanto, en su calificación hay que atender a conceptos éticos y jurídicos que pueden ser variables para cada territorio o cada persona.

“En el derecho comparado, la Unión Europea, se aleja de dar recetas y ha desarrollado una política preventiva para las empresas y de responsabilidad para el usuario, en tanto que Estados Unidos, ha diseñado una regulación específica e impone severas sanciones al que divulga material indecente u ofensivo al cual pudieran acceder los menores (Ley de Decencia en las Telecomunicaciones de 1996), lo que ha suscitado en

dicho país una fuerte polémica por estimarse que atenta contra la libertad de expresión lo que motivó que fuera declarada inconstitucional”.¹⁸

La cuestión básica que se debe analizar es si son responsables los intermediarios de servicio de Internet que facilitan el servicio de transmisión y el de alojamiento automático, provisional y temporal de la información, o debe adjudicarse la responsabilidad a los suministradores de contenido que son los autores del material que se pone a disposición de los usuarios de las más diversas culturas e idiosincrasias, aspecto que es particularmente crítico cuando se trata de un ente virtual sin un asiento o domicilio físico establecido; En la práctica, se exonera de responsabilidad al prestador de servicios de transmisión a condición de que no haya originado él mismo la información, no seleccione al destinatario o modifique los datos transmitidos, ni impida el acceso o retire el dato.

“No desconocemos que estas funciones operativas pueden coincidir o se pueden complicar técnicamente, pero normalmente no ocurre así y el proveedor de servicios de transmisión y acceso (ISP) es ajeno y solamente deja pasar al proveedor de contenido (este último puede variar desde pornografía infantil hasta recetas médicas), o sea, no lo selecciona, no interviene o modifica la información ni mucho menos la puede censurar, salvo que cuente con autorización judicial. Por lo tanto, no puede responder por ella. La misma hipótesis de adjudicación de responsabilidad es aplicable si el sitio introduce voluntariamente enlaces o links a sitios o páginas web de terceros que tengan

¹⁸ Muñoz Machado, Santiago. **La regulación de la red, poder y derecho en internet**. Pág. 17

contenido visual claramente ilícito o capaz de ofender y dañar al usuario que lo visita, lo cual también puede engendrar responsabilidad”.¹⁹

Se puede perseguir y sancionar de un modo efectivo la circulación de los contenidos nocivos o ilícitos en el denominado ciberespacio, si se aspira a que los usuarios, especialmente los menores de edad, se mantengan protegidos de estos contenidos ilícitos y nocivos, no es en Internet donde hay que producir el cambio fundamental, ya que obviamente hay un problema ético global detrás de esta sociedad de la información.

2.4. Derecho a la intimidad

Este es el derecho de la persona a que su intimidad no sea vulnerada por un abuso de los medios informáticos.

“En el espectro mundial, los gobiernos de Estados Unidos, Canadá y la Unión Europea han venido desarrollando políticas para la protección de la privacidad en materia de Internet, identificando algunos principios básicos para desarrollar el lineamiento de la regulación jurídica emergente sobre esta materia. Para los efectos de hacerlos exigibles, deberán desarrollarse mecanismos que permitan su salvaguarda, sea por la vía de la protección brindada por la autoridad, con la consecuente acción para el caso de contravención, o mediante políticas de privacidad o programas de autorregulación

¹⁹ Fernández Rodríguez, José Julio. **Lo público y lo privado en internet: intimidad y libertad de expresión en la red**. Pág. 54

sustentados por las propias empresas e informados en las páginas web respectivas. En este último caso, las empresas deberán contar con una licencia otorgada por la autoridad pública, la que resguardará que la información entregada sea cierta, clara y permanente”.²⁰

Los principios que protegen la privacidad en internet son:

-La información; es fundamental notificar al usuario en forma previa, clara y detallada, que la entidad o empresa recopilará información personal, el uso que se le dará, el medio en que ésta se acopiará, y si los consumidores deberán ser requeridos para hacer uso de ella.

- El principio de opción: el cual permite al usuario decidir si la información recolectada de sí mismo será utilizada para propósitos distintos del que le fue señalado y aceptado originalmente.

- El concepto de acceso: se refiere a la facultad individual del consumidor para acceder a la información de sí mismo recolectada por el servidor, de manera tal de poder constatar su existencia, corregirla o complementarla y/o eliminarla, si así lo desea.

- El principio de seguridad: se refiere a la obligación de quien acopia la información personal de protegerla ante un acceso, uso y exhibición no autorizados, como asimismo respecto de su pérdida o destrucción.

²⁰ **Ibíd.**, Pág. 55

- La exigibilidad: para el cumplimiento sustantivo de los principios antes mencionados, está dada por la regulación jurídica y el régimen sancionador que la autoridad pública debe aplicar en esta materia.

Existen leyes mal llamadas de protección de datos de carácter personal, ya que en realidad lo que defienden son los derechos de las personas a su intimidad en un principio evitando su conocimiento y almacenamiento y posteriormente facilitando al interesado el acceso a sus propios datos.

“En cuanto a la regulación, las técnicas legislativas que han sido empleadas son diferentes; ya sea mediante un enfoque constitucional (Portugal Artículo 35, 1976; España Artículo 18, 1978...); a través de un tratamiento globalizador, mediante una Ley General de Protección de datos (Francia, Alemania y Suecia); efectuando un tratamiento de carácter sectorial con normas diferenciadas para el sector público y privado (Dinamarca y Estados Unidos); mediante un tratamiento específico de cada caso (Ley Sueca de información crediticia, 1973). Las leyes a partir de ahora, inciden fuertemente en la seguridad de la información, tanto en los propios bancos de datos como en las líneas de comunicación proponiendo medidas de seguridad tanto físicas como lógicas e impulsando el uso de claves criptográficas”.²¹

No todos los países tienen el mismo grado de protección, inclusive en algunos se puede decir que existe cierta permisividad; por ejemplo: en Estados Unidos de América, prima

²¹ **Ibíd.**

el derecho a la transmisión de información sobre el derecho a la privacidad de los ciudadanos. La Unión Europea, con el deseo de armonizar las leyes de protección de datos de los diferentes países, aprobó en 1995 la Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y la libre circulación de éstos.

2.5. Regulación internacional de internet

El uso de internet como un medio por el cual las sociedades, los gobiernos y en general los individuos han logrado comunicarse, intercambiar información, comprar diversos artículos, conocer lugares virtualmente, realizar pagos de impuestos, etc.; ha llevado a la mayoría de los Estados ha adoptar una postura sobre este tema, mismo que ha salido de todo marco jurídico de regulación tanto interna como internacional y que por tanto requiere un tratamiento especial tendiente a establecer un instrumento jurídico que contenga las reglas básicas para el tratamiento de este fenómeno.

Lo anterior, se hace necesario puesto que a nivel internacional no existe ningún Tratado que regule el uso de internet y que pueda por tanto dar los instrumentos para la tipificación de delitos, para establecer claramente las responsabilidades de las empresas prestadoras del servicio y los usuarios, el acceso a la información, la clase de información que circula en la red y que sirva principalmente de guía a los Estados sobre cómo manejar el internet a nivel interno.

a) Organismos internacionales: Respecto a la regulación internacional cabe señalar que los Organismos Internacionales trabajan en forma conjunta, aunque tienen objetivos particulares a seguir.

“En la Organización para la Cooperación Económica en Asia-Pacífico (APEC) la regulación de los Proveedores de los Servicios de Internet (ISP’s); se enfoca al examen de las tarifas de cobro de los ISP’s (de acuerdo a la región en la que laboren, el desarrollo, funcionalidad y condiciones de los proveedores) y lo relacionado al tráfico de los flujos de información. La Unión Internacional de Telecomunicaciones (UIT) trata de englobar todos los problemas como órgano máximo en materia de telecomunicaciones. Se enfoca principalmente en los problemas del sistema de nombres de dominio. La Organización para la Cooperación y el Desarrollo Económico (OCDE) es la más activa, aborda en términos generales la problemática del ciberespacio, esto es, desagrega todos los componentes del fenómeno y los estudia por partes y por países, identifica los puntos clave, elabora propuestas y las ofrece a sus países miembros”.²²

En materia de comercio electrónico, el documento de regulación lo constituye la Ley Modelo de las Naciones Unidas para el Derecho Mercantil, dado que es el área con mayor avance. Ésta ley estipula la importancia y trascendencia del comercio electrónico y su regulación.

²² Hance, Olivier. **Leyes y negocios en internet**. Pág. 31

En el 2004 la Organización de las Naciones Unidas –ONU- llevó a cabo un foro para la gobernabilidad de Internet, así como asegurar que los modelos de gestión de este nuevo medio sean inclusivos y participativos, puesto que se consideró el gran potencial que tiene Internet, no sólo como un instrumento de intercambio y de comunicación humana, sino en el desarrollo social y económico.

“En lo que respecta a la región latinoamericana se llevó a cabo la Conferencia del Registro de Direcciones de Internet para América Latina y el Caribe (LACNIC) organización que administra los recursos de internet en América Latina y el Caribe en donde se realizó un debate que concluyó con un llamado a la mayor internacionalización del gobierno de la red de intercomunicación electrónica. Se aclaró que no existe un gobierno de Internet ya que ésta es ingobernable como un todo; Por lo tanto considera que no hay una organización o un único ámbito para los múltiples aspectos relacionados a la red (comercio electrónico, propiedad intelectual, comunicaciones, derechos humanos, educación, privacidad y otros), ni un único organismo donde se tomen decisiones o se fijen estándares, en consecuencia, no existe el tan famoso gobierno de internet. La Comisión Europea aprobó el 26 de noviembre de 1997 la propuesta de un Plan de acción para el uso seguro de la red de la Unión Europea, el plan identifica las áreas en las que es necesaria la aplicación de medidas concretas que recibiesen el apoyo de la Unión Europea”.²³

Entre las áreas de actuación figuran las siguientes:

²³ Esteve González, Lydia. **Derecho e internet**. Pág. 13

- La creación de una red europea de centros de asistencia para recibir la información de aquellos usuarios que localicen contenidos en Internet que consideren ilegales.
- El desarrollo de sistemas de autorregulación por parte de los proveedores de acceso, proveedores de contenidos y operadores de redes.
- El uso de sistemas internacionalmente compatibles para clasificar y filtrar contenidos y proteger a los usuarios, especialmente a los niños, de contenidos no deseables.
- La aplicación de medidas que incrementen el nivel de alerta de padres, profesores, niños y otros usuarios, y que les ayuden a utilizar las redes de manera selectiva, escogiendo los contenidos más apropiados y ejerciendo un nivel razonable de control.

Estos elementos permiten configurar un mundo en línea seguro y legal. Uno de los temas más importantes es la promoción de una fuerte protección de la propiedad intelectual a través del establecimiento y la ejecución de las leyes.

Considerando que el software, es uno de los baluartes tecnológicos más apreciados de la era de la información, puesto que rige el funcionamiento del mundo de los ordenadores y de internet, por este motivo y por la facilidad con la que se pueden crear copias exactas de los programas en cuestión de segundos, la piratería de software se encuentra muy extendida. Los piratas informáticos no sólo perjudican a las compañías que fabrican software, sino que, al no ser posible reinvertir el dinero que éstas obtienen en investigación y desarrollo de programas más avanzados, también perjudican a todos los usuarios. Por este motivo, cualquier forma de piratería de software (incluso una copia de un programa para un amigo) se considera ilegal.

“Sin embargo, con todo esto es importante remarcar que no se puede asimilar este control a un control en términos políticos y jurídicos sino más bien en términos económicos y técnicos. Esto lleva a entender que los únicos controles que se realizan en cuanto a internet se refiere, son los hechos por empresas u organizaciones y estos generalmente hacen referencia a aspectos de carácter tecnológico o política de expansión, entendida principalmente en términos comerciales y por tanto de mercado”.²⁴

En este sentido, es importante preguntarse si es o no posible regular el internet a nivel internacional, dado que este ha crecido y se ha desarrollado al margen de toda legislación, con un carácter aterritorial que no respeta límites fronterizos, normas locales o estatales, lo cual pone enfrente a un mundo libre e interconectado sin ningún tipo real de restricciones ni censuras.

Si se entiende lo anterior, es fácil que se pueda estar a favor de la autorregulación que pueda generarse en esta materia, empero ante un fenómeno de tal magnitud es necesario se atienda y entienda a nivel internacional bien para establecer que significa Internet para el mundo, cuales son sus ventajas y desventajas, cual es la responsabilidad de nosotros como usuarios y ver que si no se busca regular en la materia estos no tienen ninguna garantía sobre lo que se hace, ve y transfiere en Internet y por tanto no tienen ante quien plantear una queja, por lo cual el mecanismo

²⁴ **Ibíd.**

jurídico-político que debe buscarse es un Tratado Internacional, pues hasta el momento es la vía más adecuada para buscar regular Internet.

La comunidad internacional no ha planteado una postura significativa que muestre el compromiso por abordar esta materia de manera conjunta y responsable que pueda contribuir al establecimiento de una determinada legislación; sin embargo, si ha hecho alusión a la necesidad de construir la sociedad de la información, entendida como un desafío global para el nuevo milenio en la cual el acceso a Internet y a todos los recursos que de él se desprenden es un tema primordial.

El internet ha tenido y continuará teniendo –para como se vislumbra el campo de la tecnología actual- un gran impacto a muchos niveles tanto social, económico y jurídico. Estos cambios no están difiriendo demasiado de otras conmociones tecnológicas que tuvieron profundas consecuencias para la economía. La única diferencia es que las expectativas que se han generado han sido mucho más altas, porque esta red parece haberse desarrollado por un cauce distinto, y a veces contrapuesto, al de las disposiciones jurídicas -al menos tal y como se las conoce habitualmente-. Sin embargo, los países son cada vez más conscientes de la complejidad jurídica y de la importancia económica que implica el uso de este innovador medio de comunicación mundial.

Con el tiempo Internet se ha convertido en un magnífico vehículo publicitario. Cientos de empresas utilizan sus páginas para hacer publicidad de sus marcas y productos,

bien de forma directa, dejando slogans y logotipos diseminados por la red, bien organizando concursos, bien patrocinando zonas o páginas, o bien disponiendo de sus propias páginas como catálogos informativos. Otro servicio que suelen ofrecer este tipo de páginas es la telecompra.

CAPÍTULO III

3. Comercio electrónico

Por comercio electrónico se entiende, tanto a la compra de producto o servicios por internet, como a la transferencia electrónica de datos entre operadores de un sector en un mercado, o el intercambio de cantidades de efectivo entre entidades financiera, o a la consulta de información, con fines comerciales a un determinado servicio, o un sin fin de actividades de similares características realizadas por medios electrónicos; sin embargo, en un sentido amplio comprende toda aquella actividad que tenga por objeto o fin realizar una operación comercial y que es electrónico en tanto ese comercio se lleva a cabo utilizando las herramientas electrónicas de forma que tenga o pueda tener alguna influencia en la consecución del fin comercial, o en el resultado de la actividad que se está desarrollando. Por lo tanto, no se trata solo de compras por Internet, ya que se puede tratar de cualquier tipo de intercambio de información, por ejemplo a la publicidad o el intercambio de ofertas.

“El comercio electrónico distingue cuatro categorías de transacciones, empresas-empresas, empresas-consumidores, empresas-gobierno, consumidores-gobierno. A su vez, el comercio electrónico distingue dos tipos básicos, el directo y el indirecto. Este último se asimila a lo que se conoce comúnmente como ventas telefónicas, es decir, el pedido y la venta se realiza por un medio electrónico pero la entrega del bien se realiza por un medio físico, ya que el bien pasa por aduana en el caso de comercio exterior, se

mantiene el control tradicional a los fines correspondientes. La revolución del e-commerce es justamente la venta directa es decir cuando la entrega del bien también se realiza por un medio electrónico. Las transacciones financieras son un campo en el cual el producto puede ser entregado por medios electrónicos”²⁵.

El comercio electrónico permite cuatro tipos de transacciones:

- a) Usuario guatemalteco con banco guatemalteco;
- b) Usuario guatemalteco con banco extranjero fuera del sistema guatemalteco;
- c) Usuario extranjero con banco guatemalteco; y
- d) Usuario extranjero con banco extranjero fuera del sistema guatemalteco.

3.1. Medios electrónicos de pago

Las transacciones de comercio electrónico pueden ser pagadas con un medio de pago tradicional como el efectivo, cuando el bien se entrega en el domicilio pactado o en forma virtual a través de tarjetas electrónicas. Los medios electrónicos de pago serían:

- a) Tarjetas
- b) Cheque digital
- c) Dinero electrónico
- d) Cajeros automáticos
- e) Fondos transferidos electrónicamente a un punto de venta
- f) Intermediarios no bancarios, que realizan el pago.

²⁵ Gómez Segade. José Antonio, **Comercio electrónico en internet**. Pág. 34.

“Hay que hacer la salvedad de que lo que los autores denominan como dinero electrónico es en realidad el débito electrónico o monedero electrónico, es decir que existe físicamente el dinero en una cuenta bancaria que se usa o dispone en forma electrónica. Esta diferenciación es importante para añadir dos medios más para comercio electrónico, como son los cajeros automáticos y las terminales de puntos de venta, también conocidos como EFTPOS (Electronic Funds Transfer at Point of Sale), o también conocidos en algunos trabajos como POS transfers”.²⁶

a) Sistemas de pago basados en tarjetas: De todos los medios de pago mencionados, el más ampliamente difundido es el de tarjetas, en Estados Unidos de América están difundidas las tarjetas de crédito, mientras que en Europa están difundidas las tarjetas de débito. Esta difusión se debe a los siguientes motivos:

- Aceptación internacional
- Inmediata acreditación.
- Tercero pagador.

A pesar de estas ventajas tienen la desventaja de la seguridad, costos de transacción, falta de privacidad y limitación de uso. En el caso de la seguridad, las compañías están trabajando en encriptados. En el caso de costos de transacción seguirán existiendo ya que son intermediarios y es lo mismo para la privacidad, nada puede impedir que se elaboren patrones de consumo. Y en lo referido a limitación de uso, si bien en algunos

²⁶ **Ibíd.**

países como Guatemala, coinciden las personas que usan Internet con las que tienen tarjetas, esto no pasa en otros países.

Una de las grandes ventajas que poseen las tarjetas es que han trabajado activamente en los estándares de comercio electrónico y seguridad en el mismo.

“Si bien dentro de los estándares se puede mencionar a ISO, CEN de la comunidad europea, ETSI del instituto europeo de tecnologías, las tarjetas han desarrollado sus propios estándares sobre estas bases, logrando un avance significativo, así se tiene el EMV o VME, que es el desarrollo conjunto de Europay, Mastercard y Visa, sobre la base de la ISO N° 7.816. Por otra parte han trabajado con Microsoft desarrollando el STT (Secure Transaction Technology) de Visa y el SEPP (Secure Electronic Payment Protocol) de Mastercard, ambos trabajos se fusionaron en el SET (Secure Electronic Transaction)”.²⁷

También existen las denominadas tarjetas inteligentes o smart cards, esta denominación es para aquellas que no realizan ni un débito, ni un crédito, sino que su valor está dado por una carga electrónica, previa o que es posible su recarga. Esto se denomina también monedero electrónico; esas tarjetas tienen la gran ventaja de la impersonalidad del gasto.

²⁷ **Ibíd.** Pág. 37

b) Dinero electrónico: Un medio de pago sobre el cual debe hacerse énfasis es el dinero en forma electrónica. Genéricamente se menciona al volumen de movimiento de comercio electrónico como dinero electrónico. Es más se considera la desmonetización de las transacciones por Internet como dinero electrónico, sin embargo hay que hacer ciertas distinciones, se podría hablar de cuatro clases de dinero electrónico, estas serían:

- Dinero electrónico: en sentido amplio, es decir la referencia que generalmente se publica en los periódicos que comprende las transacciones realizadas sin importar el medio de pago usado.

- Dinero electrónico con tarjetas: es decir es el comúnmente usado con tarjetas de débitos, pero que físicamente está en una cuenta bancaria.

- Dinero electrónico sin tarjetas: es decir que tiene respaldo físico de una cuenta bancaria, pero que sólo se usa o existe virtualmente, como impulsos electrónicos.

- Dinero electrónico: estrictamente hablando, sería un medio de pago emitido para ser usado por Internet. Podría ser emitido por un estado soberano, pero también podría ser emitido por una empresa privada.

“Los dos primeros tipos de dinero electrónico son conocidos; Sin embargo entre el tercero y cuarto hay una diferencia filosófica. El tercero si bien es dinero virtual tiene

una convertibilidad establecida con dinero real, este el caso de Mondex y es el que se espera se popularice en las redes. Pero en el cuarto caso, hay una profunda diferencia, es el caso de Digicash y es moneda en forma electrónica y emitida en forma electrónica”.²⁸

No debe olvidarse que la emisión de moneda, una facultad exclusiva y excluyente del Estado nacional que los constituyentes le delegaron expresamente; en consecuencia, no puede delegar en particulares la facultad de emitir monedas, por lo que su emisión por parte de que una empresa privada, habilite o valide dinero en forma electrónica o en la net, vulneraría lo dispuesto por la Carta Magna guatemalteca.

Sin embargo, la emisión de moneda privada no es un concepto extraño en la red, ya que instituciones internacionales promocionan estas iniciativas. Pero estas monedas deben competir con las ya instituidas, y en general la tendencia mundial es de convergencia de monedas (caso del euro) por lo que suponer un escenario de infinidad de monedas virtuales privadas es un poco irreal.

Lo que sí seguramente se generalizará, son los sitios con fondos genuinos de bancos reales y con monedas ya instituidas. Es el caso del tercer tipo de dinero electrónico enunciado. Otro gran sector en crecimiento y con perspectivas es el uso de cambio en Internet, ya que la red permite fraccionar la moneda hasta límites insospechados, a su vez el éxito de amazon.com y otros sitios esta basado en transacciones.

²⁸ Illescas Ortiz, Rafael. **Derecho de la contratación electrónica**. Pág. 218

“Si bien en la generalidad de los países no hay previsiones respecto a esto ya han comenzado a aparecer normas específicas, en el caso de Francia, cualquier esquema de dinero electrónico debe ser remitido al Banco Central. En Holanda se considera a los emisores privados como instituciones de crédito y deben tener autorización del Banco Central. En Italia los emisores de moneda electrónica deben ser instituciones de crédito”.²⁹

3.2. Las características generales de los contratos a través de internet y la nueva forma de concebir la contratación

Las nuevas tecnologías afectan a todos los ámbitos de la vida social, modifican algunas de las costumbres o facilitan el acceso o el disfrute de nuevos servicios. Puede afirmarse que todo lo que se encuentre cercano con el universo de la red de redes tendrá consecuencias que producirán efectos sobre las personas, de hecho, ya lo producen.

“No obstante ello y, concretamente respecto a la teoría general de las obligaciones y contratos, Internet no tiene porque revolucionar el sistema: seguirá habiendo obligaciones positivas o negativas, transitorias o duraderas, alternativas, facultativas, específicas y genéricas, divisibles e indivisibles, pecuniarias, líquidas e ilíquidas, mancomunadas y solidarias, unilaterales y bilaterales, principales y accesorias, puras,

²⁹ Rodríguez, Jacobo. **El futuro de la moneda en la era de la información.** Pág. 24

condicionales y a plazo; como correlato, seguirán produciéndose cumplimientos e incumplimientos”.³⁰

A su vez, en materia de contratos, se seguirá teniendo, como elementos o requisitos esenciales de los mismos, el consentimiento de los contratantes, el objeto cierto que sea materia del contrato y la causa de la obligación que se establezca.

Las actuales clases de contratos (y otros atípicos que puedan surgir), sus efectos, transmisión y extinción encuentran una acogida pacífica en las nuevas tecnologías. A pesar de ello, y por el principio de la practicidad del derecho, se producen retos nuevos, que significan formas distintas de encarar los problemas concretos, como ejemplo se puede citar lo que ocurre con el consentimiento: no faltará en ningún contrato pero, por la propia naturaleza del comercio electrónico, se otorgará sin la presencia de las partes, originando con ello, la necesidad de aplicar medidas de identificación extras para asegurar la identidad de los contratantes.

“Por otro lado, es notorio como en el hecho de la vida actual, la contratación electrónica soporta una regulación jurídica inadecuada en cierta medida, bien porque surgen figuras y operadores o relaciones que carecen de regulación (aunque la tendrán con el tiempo) bien porque el ordenamiento jurídico vigente tiene determinados desajustes. Estos desajustes se encuentran en algunas normas contractuales generales y de

³⁰ Tellez Valdes, Julio. **Derecho informático**. Pág. 21
42

protección de los consumidores, en algunas normas procesales y en normas que deben propender a dar protección penal al sistema”.³¹

3.3. Puntos débiles de las transacciones electrónicas

Si el comercio electrónico es aquella comercialización en la que se utiliza la herramienta electrónica, no en todos los casos intervienen los modernos medios de comunicación telemáticos; no obstante, hablar de contratación electrónica supone que, en múltiples casos, ésta se realice mediante una red de telecomunicaciones y, en particular, por ser la más utilizada, conocida y distribuida, mediante el uso de internet. Es así que se plantea la contratación por Internet, lo que obliga a precisar los aspectos que inciden en ésta contratación por la influencia que pueden tener en los medios de comunicación.

La circunstancia de que los contratantes se encuentren distantes en este tipo de contratación y las características que influyen en la formación de la voluntad, debido a que no existe presencia física entre las partes, hacen que esta contratación resulte, jurídicamente particular.

La contratación que se realiza entre ausentes, a distancia, posee una particularidad que la hace depender del medio de comunicación que se utilice. Naturalmente que no es lo mismo, por poner un ejemplo, la contratación perfeccionada a través del correo como medio de comunicación, que aquella en la que se utiliza la comunicación telefónica; ello

³¹ **Ibíd.**

lleva con facilidad a exponer que no es lo mismo tampoco cuando se utiliza como medio la comunicación telemática en la que confluyen características que pueden plantear diversas cuestiones jurídicas.

Si se acepta que toda contratación conlleva un acuerdo de voluntades para que llegue a perfeccionarse y que, en ocasiones, la contratación puede realizarse telemáticamente sin la intervención de la persona en la formación de la voluntad, conllevando aspectos de seguridad en la transmisión, de identificación de las partes y de autenticación del contenido, así como, en su caso, de integridad y conservación de los documentos que se generen por medios electrónicos.

Los problemas que se presentan con la intervención de los medios de comunicación telemáticos se centran, básicamente, en la seguridad de que se está contratando con quien se cree que se está contratando, de que lo que se recibe es lo mismo que la otra parte ha querido enviar y que se ha recibido completo; a partir de esta situación, los requisitos generales que debe reunir la contratación electrónica, son dos: debe ser capaz de suministrar prestaciones técnicas o tecnológicas suficientes, seguras y sencillas. Al tiempo que debe contar con una regulación jurídica adecuada.

Esta cuestión de la seguridad se ha afrontado tanto en redes abiertas como cerradas, utilizando sistema de encriptación, claves de acceso (fijas o variables) y diferentes programas o protocolos. En definitiva, está en el ambiente la sensación de que la

contratación por Internet crecerá de forma espectacular cuando el sistema sea seguro y sencillo.

“El principio jurídico más básico vulnerado es el de seguridad jurídica, reconocido en la Constitución. Obviamente se lesiona este principio si se produce un incumplimiento de las formalidades prescritas por la ley a cualquier tipo de documentos, sean éstos de carácter privado o público. Es sabido que éstos no se pueden dar por existentes si no hay certeza sobre datos tan fundamentales como son los referidos a los nombres del emisor o receptor, tampoco si no se tiene seguridad sobre su contenido o sobre la fecha de emisión y recepción. Desde una óptica puramente legalista, la pregunta que se suscita es si pueden todos los contratos perfeccionarse mediante la utilización de medios electrónicos. A este respecto, debemos partir de la libertad de forma contractual en el ordenamiento jurídico y del llamado principio de autonomía de la voluntad de los contratantes; si atendemos a ello, en principio es posible celebrar cualquier tipo de contrato y que se perfeccione mediante la utilización de medios telemáticos; ahora bien, esto no siempre es así ya que habrá que atender a características especiales y formalismos que normativamente son exigidos a determinados contratos o relaciones contractuales”.³²

Es por ello que no todos los contratos pueden realizarse y llegar a perfeccionarse mediante la utilización de medios telemáticos, ya que existen algunos tipos de contratos que, por imperativos legales, exigen algún formalismo que impide su perfeccionamiento

³² **Ibíd.**

mediante ésta vía, por lo que debe haber una reforma legislativa para que los mismos puedan realizarse.

No obstante lo anterior, hay gran cantidad de contratos que se perfeccionan a través de medios telemáticos y que requieren de seguridades en lo que a la seguridad jurídica respecta, ésta exige, por su parte, tanto la comprobación de la identidad de los intervinientes, como la autenticación del contenido e integridad del mensaje que tendrán adecuada respuesta con el cifrado del texto y la utilización de técnicas criptográficas.

Con todo ello, los problemas que se plantean no son estrictamente jurídicos, sino de posibilidad de garantizar la seguridad necesaria en todos los ámbitos, y en todas las fases, de la contratación electrónica.

“Una de las modificaciones que necesariamente lleva consigo la aplicación de las nuevas tecnologías al universo contractual, es la relativa al concepto de documento, palabra que debe dejar de identificarse con papel escrito. Cada vez, serán más corrientes las referencias a documentos sobre soportes distintos al papel (discos magnéticos, chips, etc.) de modo ya que no se puede equiparar al documento con el papel escrito y firmado. Además, existe otro concepto que es el de la desmaterialización de los documentos. En definitiva, se trata de colocar al documento electrónico en condiciones de hecho y de derecho similares a la de los documentos sobre soporte papel, de modo que al documento electrónico no se exija más que al documento escrito.

Tanto el documento electrónico como el documento escrito tendrán la misma protección y ambos sufrirán falsificaciones y hasta resulta probable que el documento electrónico sea más difícil de falsificar que su antecesor. Lo mismo sucede con las firmas; la firma autógrafa no es la única manera de signar, también pueden servir las claves, códigos, etc., de manera que tendremos firma autógrafa o escrita y firma electrónica”.³³

Con referencia a la posición de las partes, existen dos matices a tener en cuenta respecto a la contratación electrónica. Por un lado, existe una posible situación de inferioridad del cliente/consumidor; por el otro, los riesgos para la entidad financiera de la contratación por Internet resultarían mayores.

La primera de las cuestiones señaladas se evidencia en los contratos de adhesión, en donde las entidades son predisponentes, no obstante, esta circunstancia no varía de la actual. Pero a ello, debemos adicionarle que, la mayoría de los clientes tiene escasos conocimientos informáticos, lo que trae como consecuencia una necesaria desigualdad técnica. Asimismo, también juega en contra del consumidor el carácter compulsivo que este tipo de contratación intrínsecamente tiene enraizado.

Respecto a los riesgos de la entidad en la contratación, parte de la doctrina entiende que no tienen porque ser mayores a los derivados de la contratación tradicional. Sin embargo, es posible que se incremente la responsabilidad de las empresas o entidades

³³ Illescas. **Ob. Cit.** Pág. 224

en la dirección de la responsabilidad objetiva o de la diligencia debida de un profesional experto.

Respecto a cuándo y cómo se perfecciona el contrato, ambos tienen gran importancia en la contratación electrónica, dado que habrá que distinguir si se trata de una contratación entre presentes o entre ausentes, por el significado que puede tener en el momento de fijar la ley aplicable y la jurisdicción.

Existen tendencias orientadas a revisar y modificar la regulación sobre la jurisdicción, ejecución y entrada en vigor, competencia judicial y legislación aplicable, en los contratos realizados a través de medios telemáticos, ajustándola a la legislación del país de destino, lo que significaría que cualquier entidad que ofertara sus productos o servicios por Internet debe estar en condiciones para cumplir todas las legislaciones de todos los países, aún cuando, en la práctica, pueda resultar imposible y, consecuentemente, limitaría el desarrollo del comercio electrónico y el mercado interior sin fronteras, en perjuicio de los ciudadanos en el mundo.

“El tratado de Bruselas, consideraba como legislación aplicable la del país de origen. Así, si los usuarios o consumidores tuvieran derecho a recurrir a los juzgados y tribunales de su propio país, se dificulta el desarrollo del comercio electrónico ya que todas las entidades que ofrecieran algo por Internet tendrían que someterse y adaptar sus ofertas a todas las legislaciones nacionales, lo que puede resultar de difícil cumplimiento. En toda la normativa relativa al comercio, en el dominio de la misma priva

el soporte en papel escrito. No obstante ello, la situación de España es más ventajosa (al igual que Alemania) que tienen normado el tema de la firma digital. Además, existe una obligación genérica de conservar los documentos en soporte papel, debidamente ordenados durante seis años”.³⁴

3.4. El contrato marco

La mayoría de los operadores del comercio electrónico no tienen experiencia, tanto en lo que respecta a la utilización de los medios técnicos como en el resultado de ese uso; ello por carecer de antecedentes comerciales que señalen el camino a seguir. Es por dicha razón que un contrato marco, con carácter previo al inicio de las relaciones telemáticas, es de una ventaja ordenativa trascendental, sobre todo cuando estas van a ser de contratación masiva ya que este tipo contractual resolverá muchos inconvenientes tales como:

- Recogería los derechos y obligaciones concretos de las partes en relación con los contratos y operaciones que se pretendan realizar por vía telemática o electrónica (ya sea por medio de Internet u otras redes).
- Determinaría el uso o conservación de la informática o telemática en la realización de tales contratos y operaciones (incluso podría especificar las características técnicas de unos y otras).
- Prestablecería los sistemas de identificación o constancia que van a emplearse.

³⁴ **Ibid.**

- Incluiría el pacto de liquidez, con el fin de dejar sentados los criterios que, en su caso, se utilizarán para determinar las cantidades líquidas que cada parte acredite frente a la otra.

Además de lo hasta aquí expuesto, no puede omitirse los siguientes puntos de análisis, a saber:

- La normativa aplicable en este tipo de operaciones difiere en el comercio entre empresas que en supuesto en que intervenga la figura de un consumidor, dado que esa normativa será más rígida en el segundo caso, para la mejor defensa de la parte débil del contrato.
- Los requisitos básicos que debe reunir un contrato celebrado en Internet serán los relativos a la información previa tales como: Identidad del proveedor, características del producto, precio, forma de pago, gastos de transporte, etc., plazo de ejecución del contrato, regulación del pago anticipado o mediante tarjeta y el derecho irrenunciable de desistimiento o resolución.

Manifestar de nuevas tecnologías en la actualidad, entraña un claro riesgo de desactualizarse en el corto período, no obstante ello, puede realizarse una breve reseña del panorama actual de la contratación electrónica en el sistema financiero. Es así que, respecto a las operaciones de pasivo, el empleo de las nuevas tecnologías no plantea problemas y se realizan con habitualidad.

En lo que se refiere a las operaciones de activo, las mismas se limitan a préstamos, descubiertos u operaciones análogas escaso valor y asociadas al uso de algún tipo de tarjeta de crédito o débito.

Las operaciones que se realizan frecuentemente a través de Internet en las oficinas virtuales de las entidades de crédito son las siguientes:

- Información general: solicitudes, ofertas en general, información sobre productos, sin olvidar la banca móvil que permite mediante el uso de tecnología para acceder a Internet desde el teléfono móvil.
- Consultas de saldos y últimos movimientos, peticiones de talonarios, consultas sobre cheques, obtención de extractos detallados y realización de transferencias.
- Tarjetas: consulta de saldos, consulta de operaciones, cambio de la cuenta asociada, solicitud de cambio de límite o modificaciones temporales del mismo, comunicaciones de robo extravío y variaciones en las formas de pago.
- Fondos de inversión: Consultas de saldos y del valor de las participaciones, consulta de últimos movimientos, aportaciones adicionales y reembolsos.
- Valores: Consulta de cotizaciones, consultas de la cartera propia, consulta de los últimos movimientos, petición de extractos, compraventa de valores y obtención de información fiscal.
- Seguros: Información general, consultas y solicitudes, tarjetas de servicios, pago de primas y cobro de indemnizaciones y gestión de reclamaciones.

También existen operaciones que se realizan mediante el intercambio de soportes magnéticos o intercambio electrónico. Estas se utilizan para la liquidación y compensación de cheques y pagarés de cuenta corriente, transferencias, otros efectos de comercio, etc.

“En todas las operaciones mencionadas, se presente la idea de masificación, en el caso de la compensación de títulos cambiarios, esa idea está presente en su máximo esplendor; la eclosión que los mencionados títulos tuvieron en el medio trajo como consecuencia, la imposibilidad de tratar manualmente tantos documentos, y produjo la evolución de las Cámaras de Compensación hacia los Sistemas Nacionales de Compensación Electrónica (SNCE). Así, los títulos cambiarios, documentos nacidos para su circulación, ya no giran debido a que han pasado a otro medio, el electrónico: cuando se realiza un anticipo o un descuento, los mencionados títulos caen en poder de las entidades de crédito y se incorporan en un sistema electrónico. En definitiva, las nuevas tecnologías incrementan el grado de desmaterialización de estos títulos”.³⁵

Es claro que la comunicación y, por lo tanto, el comercio electrónico se extiende, día a día, a nuevos sectores de la actividad. Asimismo, resulta lógico que las nuevas tecnologías sean empleadas por los sectores en los que la masificación, sea de personas, de operaciones o de ambos factores, es más patente. En la administración pública, esos sectores son principalmente el fiscal y el sanitario; en el sector privado, se destacan las grandes empresas suministradoras de bienes y servicios. Es evidente que,

³⁵ **Ibíd.**

la necesidad obliga a buscar soluciones en las nuevas tecnologías y, por lo tanto, a desarrollarse en el medio de la firma electrónica.

“Para que tenga legalidad la firma electrónica los usuarios deben recurrir a los prestadores de los servicios de certificación, los cuales pueden ser definidos como las personas físicas o jurídicas que extienden los certificados que vinculan unos datos de verificación de firma a un signatario y confirman su identidad. La aparición de estos prestadores de servicios de certificación es lenta pero ininterrumpida y van surgiendo a medida que los sectores económicos se abren a las nuevas tecnologías”.³⁶

Es probable que no existan dificultades desde el punto de vista jurídico y que ni siquiera sea necesario acudir a elucubraciones o interpretaciones analógicas; pero lo que es seguro es que resulta necesario realizar su estudio para ver hasta qué punto al contratar con uso de nuevas tecnologías, puede incluirse sin inconvenientes en la casuística de la que se puede llamar contratación convencional, lo cual implica, necesariamente, establecer los criterios y elementos legales que deben incorporarse a la legislación vigente para que pueda consolidarse el comercio electrónico.

³⁶ Hance. **Ob. Cit.** Pág. 33

CAPÍTULO IV

4. Los fundamentos doctrinarios que definen la creación de una norma que regule el comercio electrónico en Guatemala

El desarrollo tan amplio de las tecnologías informáticas ofrece un aspecto negativo: ha abierto la puerta a conductas antisociales y delictivas que se manifiestan en formas que hasta ahora no era posible imaginar. Los sistemas de computadoras ofrecen oportunidades nuevas y sumamente complicadas de infringir la ley, y han creado la posibilidad de cometer delitos de tipo tradicional en formas no tradicionales. En los últimos tiempos, ha sido evidente que la sociedad ha utilizado de manera benéfica los avances derivados de la tecnología en diversas actividades; sin embargo, es necesario que se atiendan y regulen las cada vez más frecuentes consecuencias del uso indebido de las computadoras y los sistemas informáticos en general, así como el comercio electrónico en particular.

Es un hecho que Internet plantea numerosas cuestiones jurídicas, que se pueden agrupar de manera general en dos grandes bloques:

- a) Las cuestiones referentes a la ordenación y regulación de la red de redes; y,
- b) Las cuestiones referentes al conjunto de relaciones jurídicas que se generan a través de internet.

4.1. La protección jurídica en internet

El uso de Internet ha traído inmensas ventajas a la sociedad, empezando por el intercambio de bienes y servicios y terminando con las posibilidades de llevar educación y cultura hasta los lugares más alejados de la civilización. Esto no significa que el internet no pueda ser utilizado para fines nocivos o la comisión de delitos. Las libertades de expresión e información existentes en Internet requieren de una protección jurídica que incluya los siguientes aspectos:

- La dignidad humana frente al peligro que representan las páginas web que incitan a la discriminación racial, cultural o social.
- La niñez de cara a la difusión de la pornografía o de formas extremas de violencia
- La propiedad intelectual frente a la distribución no autorizada de trabajos científicos, musicales o programas de cómputo.
- La seguridad nacional, que se ve amenazada cuando se difunden instrucciones para el armado de bombas o producción de drogas.

En el desarrollo de la red de redes se han perfilado varios campos de posible conflicto debido a la ausencia de reglas suficientemente claras. Hay quienes consideran que basta con legislar, aunque el problema es de mayor complejidad debido a las características únicas de internet.

Las conductas que se llevan a cabo con ayuda de la red, no están exentas del cumplimiento de las normas jurídicas, es por eso que Internet debe ser objeto de estudio por parte del derecho en razón de que es un sistema por el cual se establecen relaciones de distinto tipo entre seres humanos; su uso para perpetrar delitos, no necesariamente depende de las redes informáticas, sino que éstas son utilizadas como herramientas.

“Desde que surgió, Internet parece haberse desarrollado por un cauce distinto, y a veces contrapuesto, de las disposiciones jurídicas. Los estudiantes y profesores que le confirieron un trato informal tenían escaso interés en establecer normas que podían limitarla. Cuando se hizo necesario establecer reglas para dictar el tráfico de mensajes y evitar conflictos entre sus autores y destinatarios, se prefirieron los códigos de comportamiento ético. No hacía falta mayor regulación. A medida que ganó presencia social y cultural, y sobre todo una significativa influencia económica, en Internet aumentaron los conflictos, y para algunos de sus usuarios, especialmente los gobiernos, la sensación de que hacían falta reglas especiales para regular el disperso universo de mensajes y espacios que es Internet, lo mismo en el empleo de recursos como el correo electrónico que en el sitio de sitios que constituye la red electrónica mundial”.³⁷

³⁷ Villanueva Romero, Sandra. **La organización internacional ante el derecho y regulación del ciberespacio**. Pág. 88

4.2. Situación legal de internet en Guatemala

En el caso guatemalteco, la legislación sobre internet promulgada hasta este momento ha sido limitada y se encuentra está centrada en los siguientes puntos:

- a) facilitar el uso de la firma electrónica, a través del Decreto 47-2008 Ley de para el reconocimiento de las comunicaciones y firmas electrónicas; y
- b) la regulación de delitos informáticos, los cuales se adicionaron al Código Penal vigente a partir del Decreto 33-96.

De ambas regulaciones la que se orienta hacia el presente tema de tesis es el primero, puesto que con la vigencia del mismo, as transacciones o documentos electrónicos adquirirán certeza jurídica.

La Ley, que fue aprobada por el Congreso de la república de Guatemala, el 19 de agosto de 2008, es una manera de representación y confirmación de la identidad de una persona en el medio electrónico, a través de datos únicos encriptados (transformados en códigos), que la hacen difícil de plagiar. El Decreto establece un conjunto de reglas generales aceptables en el ámbito internacional, que permitirán el desarrollo seguro de las vías del comercio electrónico. La entrada en vigor de la firma electrónica permite, tanto a grandes o pequeñas empresas, así como a usuarios individuales, comunicarse en la red con la seguridad de que sus comunicaciones no serán interceptadas.

Con la implementación de esta nueva Ley, Guatemala se unió a El Salvador y Costa Rica, los otros dos países que la han instaurado; asimismo, se tiene un respaldo jurídico para apoyar el desarrollo del comercio electrónico en Guatemala, especialmente para que las pequeñas y medianas empresas nacionales ingresen al comercio electrónico.

A pesar de este pequeño avance, se requiere crear en el consumidor la confianza en el nuevo canal de negocios; para ello éste debe sentir la misma tranquilidad que percibe cuando adquiere bienes o servicios en el mundo real; sin embargo, los portales o sitios virtuales, incluso de grandes organizaciones, guardan silencio sobre información tan básica como puede ser la ubicación geográfica de la misma, sobre el responsable de atender las peticiones, quejas y reclamos de los consumidores, sobre los mecanismos o escenarios en los cuales se puedan ventilar las diferencias nacidas de la adquisición de bienes y servicios relacionadas con las garantías de estos, entre otros aspectos.

Esta confianza es fundamental, a partir de que el crecimiento del comercio electrónico está determinado por el consumidor, y para lograr la confianza de éste se requiere garantizar sus derechos, y concienciar a quienes comercializan bienes y servicios en la red que éstos tienen deberes y obligaciones respecto de estos protagonistas. Por su parte, es hora que el Estado modernice las disposiciones relacionadas con el derecho del consumo, que el consumidor encuentre respuestas ágiles y oportunas en la autoridad competente en esta materia; sin estos cambios será lento el crecimiento de esta nueva forma digital de hacer negocios.

En el país la expansión generalizada de Internet debe ser acompañada de una ley específica que aborde los elementos del comercio electrónico, los delitos informáticos, el mecanismo de concesión de nombres de dominios, que establezca los mecanismos requeridos para un uso seguro y confiable de las telecomunicaciones.

Para concretar las últimas razones de la legislación sobre internet falta también por decir que su contenido debe responde no sólo al hecho de la red de redes sino también, a la circunstancia de que existen dificultades técnicas y jurídicas observadas en el funcionamiento de los mecanismos básicos de Internet que aconsejan la adopción de determinada legislación.

Esta circunstancia es destacable cuando, como en la actualidad, la sociedad mundial se encuentra en la fase de aparición de fenómenos desconocidos como el hecho de que en un instante, mediante Internet, puede comunicarse, utilizando el habla, la escritura y las imágenes, con personas que desarrollan su vida en otros lugares del mundo.

El fenómeno requiere, como cualquier otro, una regulación normativa que prevea tanto su implantación como la solución de los diferentes problemas sociales que el mismo pueda causar. En la propuesta de solución han de intervenir, como en la del resto de los problemas sociales, expertos en Derecho y en otros conocimientos y técnicas. Todo ello, sin dejar de lado la premisa mediante la cual se entiende al derecho como una ciencia práctica que, sobre la circunstancia concreta, desarrolla la normativa positiva a aplicar.

La norma debe consagrar un conjunto significativo de dominios que pretenden establecer un ciclo de seguridad lo más completo posible, advirtiendo que no todos ellos tienen impacto jurídico. Desde ya es importante mencionar que el enfoque que se propone se alimenta tanto de normatividad nacional como internacional, así como de otras fuentes del derecho, en razón de la escasa legislación que existe.

El enfoque basado en procesos para la gestión de la seguridad de la información, es el método a seguir en la definición de la norma, lo cual permite estimular a los usuarios a hacer énfasis en la importancia de:

- a) Comprender los requisitos de seguridad de la información del negocio, y la necesidad de establecer la política y objetivos en relación con la seguridad de la información;
- b) Implementar y operar controles para manejar los riesgos de seguridad de la información de una organización en el contexto de los riesgos globales del negocio de la organización;
- c) El seguimiento y revisión del desempeño y eficacia del sistema de gestión de seguridad de la información, y
- d) La mejora continua basada en la medición de los objetivos.

4.3. Los fundamentos jurídicos que informan a una norma sobre comercio electrónico en Guatemala

La comprensión de la finalidad y de los procesos involucrados en la aplicación de la norma es un requisito fundamental para la adecuada contribución desde el derecho al

sistema de gestión de seguridad de la información en una organización, tema que no puede obviar el operador jurídico que como consultor intervenga.

Al respecto se identifican seis grandes temas dentro del comercio electrónico que deben ser normados desde la perspectiva jurídica:

- a) La protección de datos personales;
- b) La contratación de bienes informáticos y telemáticos;
- c) El derecho laboral y prestación de servicios, respecto de la regulación de aspectos tecnológicos;
- d) Los servicios en línea;
- f) La propiedad intelectual; y
- g) El tratamiento de los incidentes informáticos.

El punto de partida para la gestión de la seguridad de la información dentro de una actividad comercial en la red, se encuentra en la política que se formule; la misma habrá de definir el marco tecnológico, gerencial, logístico y jurídico dentro del cual se administren los activos de información, que permita brindar apoyo y orientación a la dirección con respecto a la seguridad de la información, de acuerdo con los requisitos del negocio y los reglamentos y las leyes pertinentes.

En un medio en el cual la legislación aplicable a los problemas propios de las tecnologías de la información y las comunicaciones es escasa cobra mayor importancia el contenido y desarrollo de la política que en esta materia se formule en una ley

específica. Adicionalmente, la presencia de las compañías en diferentes sectores económicos implica el cumplimiento de una serie de disposiciones legales, lo que supone dificultades al deber armonizar estas disciplinas particulares con las novedosas tendencias del derecho informático.

Desde esta perspectiva, la política de seguridad que se formule en la ley puede ser el punto de encuentro de todas las disposiciones legales y reglamentos a que pueda estar sometida en desarrollo de la actividad económica en diferentes países. Esta situación ofrece un espacio interesante de autorregulación, en la medida que la legislación podrá incorporar las mejores prácticas o estándares en una determinada materia; situación, que por demás, facilitará el cumplimiento de la normatividad que deba ser similar en diferentes países en los cuales tenga presencia, siempre que las mismas no sean contradictorias.

El reto para los encargados de redactar la legislación es tomar en cuenta la necesaria protección de la información a partir de comprender que la política de la seguridad tiene la necesidad de considerar aspectos tecnológicos que impactan la ciencia jurídica, y viceversa; por tanto, de manera permanente habrá de revisarse y ajustarse en las guías o directrices que desarrollan la política de seguridad, la evolución del derecho predicable a los asuntos jurídicos y tecnológicos allí contemplados.

La formulación de la política de seguridad informática en la legislación seguramente habrá de ser diferente, pues la misma debe ser formulado sobre la base de los múltiples

riesgos que pesen sobre la información, así como sobre la clase de activos involucrados, y las personas que tengan acceso a la información; factores que no pueden ser dejados al margen de una adecuada gestión de seguridad de la información.

La protección de datos personas, es un tema de gran trascendencia para los seres humanos en la sociedad de la información, aunque todavía tiene poca relevancia en el medio guatemalteco, a pesar de constituir un derecho fundamental contenido en la Constitución Política. Todavía se carece de una ley que regule de manera integral el derecho fundamental a la intimidad y al habeas data, que permita garantizar las libertades públicas de los ciudadanos y en esa medida ser vistos como lugares seguros para la transferencia y tratamiento internacional de datos, pues se debe garantizar la protección de los datos personales y la privacidad, de acuerdo con la legislación y los reglamentos pertinentes y, si se aplica con las cláusulas del contrato.

Para el cumplimiento de este control, quizás el referente internacional más representativo en materia de Protección de Datos Personales es la Directiva 95/46/CE, la cual establece el marco de regulación para los países miembros de la Unión Europea; norma que ha sido desarrollada en cada uno de esos países, producto de la conciencia de los ciudadanos sobre el destino de sus datos y el compromiso del Estado de garantizar las libertades públicas vinculadas al derecho fundamental a la intimidad.

En este orden de ideas, para ilustrar la problemática de la intimidad y el habeas data ha de entenderse el concepto de dato de carácter personal como cualquier información concerniente a personas físicas identificadas o identificables, los cuales pueden ser generales, como nombre, domicilio y documento de identidad; hasta información sensible como ideología política, estado de salud, tendencias sexuales, credo religioso, grupo étnico, entre otros.

En la economía actual, los datos de carácter personal están sometidos a tratamientos o procedimientos técnicos que permitan recabarlos, modificarlos, bloquearlos, cancelarlos, cederlos o transferirlos a terceros, así como definir perfiles de distinta naturaleza según la información que se desee obtener, acudiendo para ello a programas de minería de datos, que terminan entregando información valiosa sobre los hábitos de consumo de un individuo.

“Esta posibilidad de que terceros puedan acceder sin control a la información personal de un individuo es lo que busca proteger el habeas data, en el sentido de que la información personal que sea confiada a una organización por su titular, esté amparada y protegida de usos ilegítimos que desconozca esa tutela constitucional que cada individuo tiene sobre su información, así como sobre los perfiles diseñados a partir de sus hábitos, comportamientos y tendencias”.³⁸

³⁸ **Ibíd.**

En consecuencia, en materia de seguridad de la información y en desarrollo de este derecho fundamental, debe procurarse la regulación legal para garantizar que toda base de datos, tenga connotación comercial o no, cuente con las medidas jurídicas, tecnológicas y físicas que aseguren su protección.

La ausencia de una norma que proteja la intimidad personal en el país, conduce a que gran parte de las bases de datos en poder de entidades públicas como privadas sean explotadas de manera ilegítima, a partir del abuso, ignorancia o desconocimiento de los derechos que tienen los individuos sobre la información confiada.

Lo anterior no pretende limitar el uso de las bases de datos, sino llamar la atención sobre la posibilidad de explotar la información dentro de unos parámetros legítimos, que atiendan los principios de consentimiento, finalidad, calidad, veracidad, conservación, entre otros, que caracterizan el tratamiento responsable de la información personal.

En materia de seguridad de la información, tratándose de datos personales, ha de recordarse que la protección a brindar se predica tanto de personas naturales como de personas jurídicas. En cumplimiento de este objetivo, la norma legal debe orientarse a que en la ejecución de proyectos contratados con terceros, no pueden dejar al margen la regulación contractual de las obligaciones que éstos deben acatar para asegurar que las medidas de seguridad de la información personal adoptadas por ella sean realmente eficaces.

“Los deberes, cargas, obligaciones, riesgos y sanciones que puedan pesar sobre los titulares de las bases de datos personales no desaparecen por encargar a terceros el tratamiento de tales datos, por el contrario, pueden incrementar el valor de estas por no haber tomado las medidas adecuadas. Igualmente, los terceros a los cuales se encomiende el tratamiento de bases de datos con información personal son responsables por el uso ilegítimo que hagan de los mismos, y en consecuencia serán responsables de los perjuicios que irroguen a los individuos titulares de los datos personales”.³⁹

El no dotar a las bases de datos personales de la seguridad y medidas de protección adecuadas por parte de las organizaciones que las poseen implica violación a un derecho constitucional, el cual puede ser garantizado a través de acciones de tutela, con el riesgo de indemnizar los perjuicios causados; asimismo, es una limitante en el comercio internacional, pues los países europeos y algunos latinoamericanos impiden la transferencia internacional de datos con países o empresas que no garanticen un nivel adecuado de protección de datos; y, por último, las sanciones que tienden a imponerse por violación a este derecho fundamental de la protección de datos personales y habeas data son muy cuantiosas en términos económicos.

Las características propias de los proyectos informáticos conducen a regulaciones no contempladas por la legislación positiva, que encuentran su fuente de regulación en la autonomía de la voluntad privada; esta realidad ratifica la concepción atípica de los

³⁹ **Ibíd.**

contratos sobre bienes intangibles susceptibles de digitalización. Por tanto, mientras se crea una normativa específica que incorpore estos elementos, la regulación de estos contratos debe ser suplida por la voluntad de las partes, los principios generales de contratación, el derecho internacional y demás fuentes, de manera que cada uno de los aspectos de la relación jurídica a ejecutar entre las partes sea definido y consignado en el cuerpo del contrato y sus anexos respectivos, advirtiendo la importancia de regular de manera independiente las diferentes prestaciones jurídicas que puedan estar vinculadas al contrato principal.

En la actualidad, además de la ausencia de una norma específica, se encuentra que los equipos de informática trabajan al margen de los equipos jurídicos dentro de las organizaciones privadas en lo que tiene que ver con los procesos de contratación informática, situación que genera una ruptura en la tarea de gestionar de manera eficaz la seguridad de los activos de la información. No son extraños los casos en los cuales aspectos sencillos como la definición de la propiedad intelectual sobre los intangibles contratados no están formalizados, o existen reclamaciones sobre la propiedad de los mismos por quienes los han desarrollado. Ante esta realidad, mientras no se legisle sobre estos aspectos jurídicos centrales, se aconseja que exista un proceso de comunicación clara entre las áreas involucradas en la contratación de intangibles

El contrato informático, como una entidad negociada independiente y autónoma, se presenta cuando el objeto de contratación recae exclusivamente sobre bienes inmateriales susceptibles de digitalización, como lo es el programa de computación, en

todas sus formas y vertientes, las bases de datos y también las obras o productos multimedia.

Los operadores jurídicos de la organización, responsables de la contratación de esta clase de bienes y servicios, han de tener en cuenta que la adquisición, desarrollo y mantenimiento de obras digitalizadas requieren de regulaciones apropiadas a la naturaleza incorpórea del objeto contratado, que exigen armonizar lo jurídico con lo técnico.

Otra buena práctica es la participación de los abogados, conocedores de la tecnología, en los procesos de negociación del proyecto informático o telemático, participación que seguramente permitirá definir de manera clara el alcance del objeto contratado, el cual en ocasiones es bastante abstracto; desechar esta práctica puede conducir a disputas futuras o costo innecesarios para las partes contratantes. En igual sentido, es válida la presencia de un operador jurídico, con el perfil recomendado, en la etapa de ejecución del proyecto, aspecto de dotará de seguridad el cumplimiento de las obligaciones pactadas.

La contratación de desarrollo de programas de ordenador o integración de sistemas de información, por las dificultades que supone dimensionar el alcance de los mismos y los valores asociados, apunta a separar las etapas de toma de requerimientos, análisis y diseño, de las etapas de desarrollo, pruebas y puesta en producción de la aplicación informática. Lo anterior permite a las partes contratantes cumplir con los tiempos

previstos, recursos económicos comprometidos, identificación plena de requerimientos, cumplimiento de las funcionalidades pretendidas al contratar, entre otros aspectos.

En términos de contratos de licencia de uso sobre aplicaciones informáticas normalmente media la entrega de la correspondiente licencia y del ejecutable que permite la instalación de sistema de información. La Ley específica que debe promulgarse debe plantear la importancia de que la organización pueda garantizar el acceso al código fuente de la aplicación cuyo uso se concede, en caso de que el titular del programa de ordenador desaparezca del mercado; situación que exige regular tal hipótesis en términos de seguridad de la información.

Igualmente, las organizaciones contratan servicios telemáticos de diversa naturaleza, como puede ser la instalación de redes de comunicaciones privadas, la gestión, soporte y mantenimiento de las mismas, así como servicios que se soporten en éstas; servicios que particularmente son provistos por terceros.

Por tanto, la gestión de redes de comunicaciones, tratándose de servicios de telecomunicaciones, aconseja adoptar medidas que vayan más allá de la prestación eficiente de tales servicios, siendo fundamental que a nivel tecnológico se adopten medidas que otorguen estabilidad a la red, ofrezcan la velocidad requerida para el funcionamiento de los diferentes equipos y sistemas, y gocen de protocolos seguros que permitan reaccionar a los ataques a los sistemas o a las redes mismas.

En los contratos de esta naturaleza no es extraño encontrar omisiones en este sentido, las cuales pueden ser resultado del desconocimiento de lo tecnológico o de la ausencia de reflexiones sobre el impacto jurídico que en materia de responsabilidad derivan para las partes involucradas. Obviar la regulación de aspectos como los mencionados puede ser fuente de conflictos o interpretaciones ambiguas sobre el alcance de las obligaciones que corresponden a las partes.

Estos asuntos han de ser regulados en los contratos telemáticos, advirtiéndose que la mayoría de ellos son de corte tecnológico, pero no por ello, se insiste, deben ser desatendidos en la relación contractual, salvo que dentro de la organización no exista preocupación por la seguridad de la información y por la gestión que la misma empresa o terceros le proporcionen.

De igual manera, las relaciones laborales son aspectos que también deben estar comprendidos en el alcance de la norma sobre el comercio electrónico. En este sentido, debe de crearse un capítulo específico denominado seguridad de los recursos Humanos, en el cual se establecerá un conjunto de controles que se deben tener presentes antes, durante y después de la terminación de la contratación laboral.

Este componente involucra las relaciones de servicios con terceros, advirtiéndose que las obligaciones aplican no sólo a las personas jurídicas o naturales con quienes se contrata, sino también a las relaciones laborales con sus empleados o relaciones de

servicios con sus subcontratistas; ello con el fin de dotar de seguridad a todas las personas involucradas con los activos de información de una organización.

Al normar esta relación laboral, se logra asegurar que todos los empleados, contratistas y usuarios de terceras partes estén conscientes de las amenazas y preocupaciones respecto de la seguridad de la información, sus responsabilidades y sus deberes, y que estén equipados para apoyar la política de seguridad de la organización en el transcurso de su trabajo normal, al igual que reducir el riesgo de error humano; de igual manera, se puede asegurar que los empleados, contratistas y los usuarios de terceras partes salen de la organización o cambian su contrato de forma ordenada. Estas situaciones de la contratación laboral o de servicios han de verse en el contexto de la relación entre los recursos humanos y los activos de la información a los que éstos tengan acceso.

Existen problemáticas nada pacíficas respecto del uso de herramientas de trabajo como el correo electrónico de la organización por parte de los empleados, en el sentido de establecer si la información allí contenida puede ser auditada por la empresa, o si tiene carácter personal, o cuál es el justo medio que pueda dar una respuesta jurídica legal a la problemática.

La tecnología permite al administrador del sistema tener conocimiento sobre los sitios de la red que un usuario visita durante su jornada laboral o de servicios, puede establecer el tiempo que éste ha estado navegando un contenido determinado;

entonces, se pregunta si esta vigilancia atenta contra los derechos de la persona. La respuesta está determinada en la definición de las políticas laborales y sus desarrollos que adopte una organización en relación con sus empleados o con los contratistas.

El uso de las herramientas tecnológicas es un proceso cultural, en el sentido que las personas desconocen los riesgos que devienen de su uso. De hecho, las fallas de seguridad o la pérdida de la información, la mayoría de las veces obedecen al desconocimiento de los riesgos que conlleva el uso inadecuado de las mismas por parte de los mismos operadores de las empresas vinculadas al comercio electrónico.

Es deber de la empresa prestadora de servicios, capacitar al personal sobre los riesgos inherentes al uso de las tecnologías de la información y las comunicaciones, dar a conocer la importancia que los activos de la información tienen, comunicar los riesgos que pesan sobre la información, las prácticas de ingeniería social de la que se aprovechan los hackers y crackers para atentar contra la seguridad de la organización; aspectos que exigen el trabajo en equipo entre los diferentes actores para consolidar un sistema eficaz de gestión de la seguridad de la información.

No menos importante es asegurarse de que las personas tengan acceso a los sistemas con base en los perfiles y autorizaciones definidas, y que a la desvinculación de éstos sean cancelados efectivamente para evitar los posibles delitos informáticos, lo cual es tarea de los administradores de los sistemas de información de una compañía.

Corresponde al operador jurídico sugerir los tópicos que se deben tener presentes en los contratos laborales y en los contratos de prestación de servicios, en lo que se refiere al manejo, administración, uso, entrega y devolución de los activos de información a los que se otorga acceso, así como a las consecuencias derivadas de la pérdida, hurto, alteración o modificación de la información entregada y confiada a estas personas.

Las reflexiones expuestas constituyen sólo la punta de iceberg de muchos otros temas que desde la tecnología impactan las relaciones laborales o de prestación de servicios, los cuales han de ser identificados y regulados, con el fin de poder integrar en la norma específica las dinámicas laborales que genera la actividad comercial en la red.

Como el comercio electrónico abarca más allá del intercambio virtual de bienes y servicios, sea éste directo o indirecto; ha de entenderse dentro de esta acepción la transmisión de información por vías digitales, sean éstas públicas como Internet o privadas como una intranet, entre otras, la norma que regule esta actividad debe garantizar la seguridad de los servicios de comercio electrónico y su utilización segura.

Conforme a este control, el cual es parte de la gestión de comunicaciones y operaciones, corresponde al operador jurídico en los temas de su competencia tener presente:

- i) Que la información que se trasmite por las redes públicas debe estar protegida contra actividades fraudulentas;
- ii) Las eventuales disputas por contratos; y

iii) La divulgación o modificación no autorizada de la información.

El referente legal que se elabore debe tener en cuenta la legalidad de los mensajes de datos y a la firma digital (que ya se encuentra regulada legalmente), la cual tiene como objetivo principal dar validez a los mensajes de datos remitidos por vías electrónicas, cosa diferente de regular las actividades de comercio electrónico que puedan celebrarse por la red.

La preocupación de seguridad de la información, respecto de las transacciones que operan a través de canales electrónicos, es que éstas cuenten con los atributos de integridad, disponibilidad, confidencialidad, y no repudio, lo cual se logra con la implementación de herramientas como las firmas digitales de clave pública y privada, de carácter asimétrico.

Las acciones que se adopten en materia de seguridad, respecto de los servicios de comercio electrónico han de atender la naturaleza del modelo de negocio, de las transacciones que se realicen, los datos que se transmitan y de los riesgos inherentes a las actividades mismas; por tanto, en cada caso habrá que identificar un catálogo de acciones a aplicar.

“En la era industrial, los activos productivos de carácter tangibles pueden ser asegurados mediante pólizas, de suerte que en el evento de un siniestro el propietario puede afectar la póliza de seguros para recuperar su inversión; hoy día, en la era de la

sociedad de la información, los activos productivos son intangibles e incorpóreos, por lo que uno de los mecanismos que sirven para proteger este tipo de bienes es la propiedad intelectual. El control que establece la norma consiste en implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legales, reglamentarios, y contractuales sobre el uso del material con respecto al cual puedan existir derechos de propiedad intelectual y sobre el uso de productos de software patentados”.⁴⁰

Bienes como el software, las bases de datos, las obras multimedia, los sistemas inteligentes son activos de valor incalculable para cualquier organización, que ameritan adoptar medidas especiales para lograr una protección eficaz.

En materia de protección del software es importante tener en cuenta que algunas legislaciones, como la europea, establecen que también es objeto de protección la documentación preparatoria de los programas de ordenador, consideración que aclara uno de los aspectos que pueden ser fuente de controversia en el sector, máxime cuando existen incumplimientos o terminaciones anticipadas de los contratos informáticos.

La protección de los bienes intangibles susceptibles de digitalización encuentra vacíos importantes en la regulación aplicable en términos de propiedad intelectual, pues la

⁴⁰ **Ibíd.** Pág. 91

asimilación que las leyes hacen a obras literarias para efectos de protección plantea cuestionamientos importantes sobre su eficacia.

En materia de seguridad de la información se requiere imprimir claridad a los contratos de desarrollo de aplicaciones informáticas en lo que respecta a la titularidad de los derechos de propiedad intelectual, los cuales en ocasiones son vagos, abstractos o no son formalizados.

Es preciso tener en cuenta que en la legislación a elaborar se requiere expresar de manera clara los derechos patrimoniales que se ceden, así como cumplir con la formalidad de la escritura pública o del documento privado con reconocimiento del contenido del documento ante notario, formalidades que en la mayoría de las veces son obviadas, con lo cual se afecta la correcta protección de activos susceptibles de digitalización.

La propiedad intelectual, en sus modalidades de derechos de autor y propiedad industrial, son temas transversales a la seguridad de la información corporativa, la cual exige de medidas que aseguren la protección de la misma.

Una organización, además de velar por asegurar la titularidad de los derechos patrimoniales sobre las obras informáticas encargadas, debe preocuparse también porque sus sistemas de información tengan las licencias correspondientes; preocupación que debe extenderse a exigir que sus proveedores cuenten con las

licencias de uso de los programas informáticos, que soportan la prestación de los servicios informáticos contratados, para lo cual su equipo de seguridad debe informar sobre la prohibición de instalar en los ordenadores programas que no tengan licencias, o programas que puedan poner en riesgos la seguridad de los sistemas o de los equipos; eventualidades que deben estar reguladas en el marco de la política laboral y de servicios que tenga la organización, sin que la misma contradiga la norma de observancia general.

El cumplimiento de las normas sobre propiedad intelectual debe ser una de las cláusulas principales en todo proyecto de comercio electrónico, pues no hay otra forma que permita extenderse a terceros la obligación de respeto sobre los derechos de propios o de terceros.

Otra recomendación es otorgar transparencia en la titularidad de los desarrollos, descubrimientos, adelantos, innovaciones y nuevas creaciones de los empleados en desarrollo de la relación laboral, los cuales pertenecen a la empresa, salvo acuerdo en contrario. Al respecto se cuestiona si las cláusulas que se acostumbran pactar en los contratos laborales, previa la existencia de los desarrollos o innovaciones, dotan de seguridad adecuada la propiedad que tiene la empresa sobre la información desarrollada, o si se requiere de acuerdos posteriores a la creación de la obra o patente.

Las normas de propiedad intelectual establecen los bienes sujetos de protección, cuáles derechos asisten a sus titulares, la duración de la protección y demás aspectos inherentes a su seguridad jurídica. Ahora bien, además de éstas, es importante en el desarrollo de proyectos informáticos tener presente que la relación entre las partes debe atender los principios de buena fe y lealtad contractual, en el sentido que debe evitarse incurrir en prácticas que la ley considera como contrarias a la sana y leal competencia.

En consecuencia, las normas sobre competencia desleal se convierten en herramientas de protección de la seguridad de la información de las organizaciones, complementando así la protección regulada actualmente sobre propiedad intelectual.

El concepto de seguridad informática es de reciente data, y tal vez fue en los últimos 15 años en los que adquirió un nombre propio. El fenómeno de atacar las redes de comunicaciones se inicia en los albores del siglo XX, cuando piratas del mundo electrónico empezaron a vulnerar los sistemas de terceros, tras la aparición de las líneas de comunicaciones telegráficas.

Una de las mayores preocupaciones de las organizaciones, y en particular de los responsables del área informática, es el tratamiento de los incidentes informáticos, es decir, de aquellas situaciones que atentan, vulneran o destruyen información valiosa de la organización, además del impacto psicológico y económico que puede generar en el

mercado accionario o en los accionistas cuando se informa sobre intrusiones y pérdidas de información en un ente empresarial.

“Quizás lo descrito en los párrafos anteriores refleja la importancia del concepto de seguridad de la información. Sin embargo, para terminar de reforzar la importancia del tema para las empresas, si aún existiese alguna duda, basta conocer un listado de los delitos cometidos por el cracker más reconocido en la historia reciente, Kevin Mitnick fue acusado de diversos crímenes: creación de números telefónicos no tarificables; robo de más de 20,000 números de tarjetas de crédito; precursor de la falsificación de direcciones; burla a la Oficina Federal de Investigaciones de Estados Unidos (Conocida como –FBI-) durante más de 2 años; robo de software de terminales telefónicos; control de varios centros de conmutación en Estados Unidos ; acceso ilegal a múltiples sistemas del gobierno estadounidense; entre otros incidentes de seguridad. Los delitos cometidos por este ex delincuente informático –quien hoy es un experto consultor en seguridad, después de purgar varios años de prisión– reflejan no sólo los tipos de conductas que configuran un incidente informático, sino también la posibilidad de que cualquier empresa sea víctima de un ataque a sus activos, sistemas o redes de información”.⁴¹

La norma debe incluir elementos legales para asegurar que los eventos y las debilidades de la seguridad asociados con los sistemas de información se comuniquen de forma tal que permiten tomar las acciones correctivas oportunamente.

⁴¹ **Íbid.**

En los asuntos de competencia del derecho en materia de incidentes informáticos, se debe promover que las organizaciones sean proactivas en la recolección de la evidencia de los mismos; en este sentido, el control establece que cuando una acción de seguimiento contra una persona u organización después de un incidente de seguridad de la información implica acciones legales civiles o penales, la evidencia se debe recolectar, retener y presentar para cumplir con las reglas para la evidencia establecidas en la jurisdicción competente.

“Se puede decir que un incidente de seguridad consiste en una conducta criminal o no desarrollada por un individuo contra sistemas de información, redes de comunicaciones, activos de información, con el fin de alterar, copiar, simular, hurtar, destruir, indisponer, bloquear y/o sabotear éstos. Estos comportamientos pueden ser desplegados por intrusos informáticos, extorsionistas, terroristas, espías industriales, usuarios de los sistemas o de las redes, ex empleados y millones de adolescentes con conocimientos meridianos en ataques informáticos”.⁴²

Para el cumplimiento de la norma en materia de recolección de las pruebas de un incidente es importante tener en cuenta que tales actividades requieren del apoyo de la informática forense. Ante la sospecha de la comisión de un incidente informático, el análisis forense permitirá recabar, procesar e investigar información procedente de sistemas informáticos, mediante la aplicación de una metodología que permita dar autenticidad a la prueba a ser utilizada en una causa judicial.

⁴² Mir Puig, Santiago. **Delincuencia informática**. Pág. 80

Frente a la presencia de un incidente informático corresponde al equipo de seguridad reaccionar frente al mismo siguiendo cuatro pasos: identificar los equipos que pueden contener evidencia del incidente acaecido; preservar la evidencia de los daños accidentales o intencionales, lo cual se logra efectuando una copia o imagen exacta del medio analizado; examinar la imagen de la copia original, buscando evidencia o información sobre los hechos que suponen la existencia de un incidente de seguridad; y por último, escribir un reporte, finalizada la investigación, en el cual debe hacerse referencia de los hallazgos a la persona indicada para tomar una decisión, bien sea a un juez o al presidente de la compañía.

El problema de la recolección de incidentes informáticos radica en aplicar protocolos que permitan un tratamiento probatorio conforme a la ley, de manera que la prueba obtenida tenga la legalidad requerida para ser aceptada en una causa judicial, sea ésta de naturaleza penal, civil, administrativa o disciplinaria.

El tratamiento que se debe realizar respecto de la comisión de un incidente informático demanda aplicar técnicas equivalentes a las practicadas para buscar la evidencia de un delito cometido en el mundo real.

En la práctica cotidiana, existen diferencias sustanciales al recabar la evidencia de incidentes informáticos, pues la prueba de tales acciones muchas de las veces pueden desaparecer o ser eliminadas por su volatilidad; característica que exige que la intervención del equipo de seguridad se realice tan pronto como se tenga conocimiento

o sospecha de la ocurrencia de un ataque a los activos de información de una organización.

Corresponde precisar que no sólo se trata de encontrar la evidencia del delito, ataque o intrusión, de carácter informático, sino que además se precisa la limpieza en la práctica de la misma, pues en caso de alterarla o desaparecer ésta, será imposible demostrar la comisión del incidente, y por esta vía, aplicar las sanciones o penas a que haya lugar, así como el resarcimiento de los perjuicios que se causen.

Ahora bien, un incidente informático puede o no tener carácter judicial, y una organización seguramente definirá por razones estratégicas hacer pública o no su condición de víctima de un ataque a sus activos de información.

Así mismo, la definición de si un incidente informático tiene carácter judicial es determinada por la tipicidad legal de la conducta del infractor; para el efecto habrá de contrastarse la misma contra los tipos penales consagrados en la legislación del país.

La recolección de la evidencia de un incidente informático, por las particularidades y características del mismo, implica la participación de un equipo interdisciplinario de profesionales capacitados en identificar, recolectar, documentar y proteger las evidencias del incidente, apoyándose en técnicas de criminalística forense, que permitan iniciar las acciones penales y civiles derivadas de la ocurrencia de estos incidentes.

Al respecto, es importante conocer los elementos legales que deben elaborarse orientados a establecer las medidas para recabar las pruebas de los hechos punibles cometidos en Internet, teniendo en cuenta la cadena de custodia, entre otras herramientas, que asegure las características originales de los elementos físicos de la prueba del incidente, desde la protección de la escena, recolección, embalaje, transporte, análisis, almacenamiento, preservación, recuperación y disponibilidad final de éstos, identificando al responsable en cada una de sus etapas y los elementos que correspondan al caso investigado.

En su conjunto, estos elementos jurídicos configuran los fundamentos doctrinarios que informan la creación de una norma que regule el comercio electrónico en Guatemala.

CONCLUSIONES

1. El comercio electrónico, en el siglo XXI, caracterizado por la sociedad de la información, implica que todas las organizaciones, sean éstas públicas o privadas, nacionales o transnacionales, cualquiera que sea el sector económico en que desarrollen su objeto social, están relacionadas con la tecnología informática y sus mecanismos de seguridad. Sin embargo los profesionales del derecho no están actualizados.
2. Las tecnologías de la información y las comunicaciones reclaman del derecho respuestas innovadoras y globales respecto de los retos que le son intrínsecos; por tanto, los legisladores, fiscales, abogados litigantes y los operadores jurídicos se han visto obligados a capacitarse para solucionar las problemáticas de la relación Informática-derecho.
3. El crecimiento del comercio electrónico en Guatemala no es representativo, por la escasa confianza del consumidor en los medios electrónicos a través de los cuales se surten las transacciones de bienes y servicios, así como un desconocimiento sobre la existencia de protocolos seguros que permiten minimizar los riesgos al suministrar información, sea esta personal o económica.
4. La legislación guatemalteca todavía resulta muy escasa para abarcar todos los aspectos legales y mercantiles vinculados al comercio electrónico y a la tecnología

de Internet, aun cuando se han llevado a cabo avances en esa línea, falta regular aspectos centrales orientados hacia los mecanismos de seguridad de las transacciones informáticas.

5. Los principales elementos jurídicos que no están presentes en la Ley que regule todos los aspectos del comercio electrónico, relacionados con la protección de datos personales, la contratación de bienes informáticos, los derechos laborales de los operadores de Internet y el respecto de la regulación de los servicios en línea.

RECOMENDACIONES

1. Debido a que la sociedad de la información avanza aceleradamente, es importante que el Colegio de Abogados y Notarios implemente diplomados para los colegiados activos, para que estos cuenten con información actualizada sobre las tendencias informáticas existentes, así como la legislación internacional y nacional que las regula
2. Debido a que las tecnologías de la información y las comunicaciones reclaman del derecho respuestas innovadoras y globales, el Colegio de Abogados debe promover un congreso jurídico para que todos los abogados y notarios expongan las propuestas de legislación más adecuada a la realidad de Guatemala respecto a las problemáticas de la relación Informática-derecho.
3. El Ministerio de Economía debe promover campañas informativas para los usuarios potenciales del comercio electrónico en Guatemala para informarles sobre la existencia de protocolos seguros que permiten minimizar los riesgos al suministrar información, sea esta personal o económica, para lograr el crecimiento de las transacciones electrónicas de bienes y servicios.
4. Las universidades del país que imparten la carrera de abogado y notario, deben crear una comisión para que elabore una propuesta de legislación que abarque todos los aspectos legales y mercantiles vinculados al comercio electrónico y a la

tecnología de Internet, que garantice la eficacia y la seguridad del usuario como del prestador de las transacciones informáticas.

5. La Universidad de San Carlos de Guatemala debe de proponer ante el Congreso de la República de Guatemala una propuesta de ley de manera que en los capítulos y artículos de la misma se incorpore la protección de datos personales, la contratación de bienes informáticos, los derechos laborales de los operadores de Internet, el respecto de la regulación de los servicios en línea y la seguridad jurídica. Por que debe existir certeza Jurídica con los contratos que se vayan a realizar por la Internet. Para que los profesionales del derecho tengan la confianza de utilizar Internet con seguridad Jurídica.

BIBLIOGRAFÍA

- ESTEVE GONZÁLEZ, Lydia, **Derecho e internet**, España: Ed. Compás, 2001.
- FERNÁNDEZ RODRÍGUEZ, José Julio, **Lo público y lo privado en internet: intimidad y libertad de expresión en la red**, México: Ed. Instituto de Investigaciones Jurídicas, UNAM, 2004.
- GUERRERO, Maria Fernanda, **La inteligencia artificial aplicada al derecho**, Italia: Ed. Revista Uno y Cero, 2004.
- GÓMEZ SEGADE, José Antonio, **Comercio electrónico en internet**, Madrid: Ed. Marcial Pons, 2001.
- HANCE, Olivier, **Leyes y Negocios en internet**, México: Ed. Mc Gram Hill, 1996.
- ILLESCAS ORTÍZ, Rafael, **Derecho de la contratación electrónica**, Madrid: Ed. Civitas, 2001.
- JIJENA LEIVA, Renato, **El derecho y la sociedad de la información: la importancia de internet en el mundo actual**, México: Grupo edi. Miguel Ángel Porrúa, 2003.
- KROL, Ed, **Conéctate al mundo de Internet**, México: Ed. McGraw-Hill, 1995.
- LOSANO, Mario G., **Curso de informática jurídica**, España: Ed. Universidad de Palma de Mallorca, 2000.
- MIR PUIG, Santiago, **Delincuencia informática**, Barcelona: Ed. Promociones y Publicaciones Universitarias, 1992.
- MONTESINOS GUTIÉRREZ, Antonio, **La sociedad de la información e internet**, Madrid: ed. Centro de Documentación, Información y Análisis Dirección de servicios de investigación y análisis subdirección de política exterior San Pablo, 1999.
- MUÑOZ MACHADO, Santiago, **La regulación de la red, poder y derecho en internet**, Madrid: Ed. Taurus, 2000.
- RODRÍGUEZ, Jacobo, **El futuro de la moneda en la era de la información**, Argentina: Ed. Cámara Argentina de Comercio, 1999
- SIYAN KARANJIT, **Internet y seguridad en redes**, México: Ed. Prentice Hall, 1995.

SU, Emilio, **Introducción a la informática jurídica y al derecho de la información**, España: Ed. Revista de la Facultad de Derecho de la Universidad Complutense, 2004.

TELLEZ VALDES, Julio, **Derecho informático**, México: Ed. Digital, 2002.

VILLANUEVA ROMERO, Sandra, **La organización internacional ante el derecho y regulación del ciberespacio**, México: Ed. Facultad de Ciencia Políticas y Sociales, UNAM, 2001.

Legislación:

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

Código Penal. Congreso de la República, Decreto número 17-73, 1973.

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