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

LA IMPORTANCIA JURÍDICA DE IMPLEMENTAR MEDIDAS DE SEGURIDAD EN LOS MEDIOS DIGITALES PARA TRANSACCIONES ELECTRÓNICAS PARA EVITAR QUE TERCEROS LO UTILICEN PARA COMETER FRAUDE EN PERJUICIO DEL TARJETAHABIENTE

AXEL DOMINGO CAZ

GUATEMALA, OCTUBRE 2012

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

LA IMPORTANCIA JURÍDICA DE IMPLEMENTAR MEDIDAS DE SEGURIDAD EN LOS MEDIOS DIGITALES PARA TRANSACCIONES ELECTRÓNICAS PARA EVITAR QUE TERCEROS LO UTILICEN PARA COMETER FRAUDE EN PERJUICIO DEL TARJETAHABIENTE

TESIS

Presentada a la Honorable Junta Directiva

de la

Facultad de Ciencias Jurídicas y Sociales

de la

Universidad de San Carlos de Guatemala

Por

AXEL DOMINGO CAZ

Previo a conferírsele el grado académico de

LICENCIADO EN CIENCIAS JURÍDICAS Y SOCIALES

y los títulos profesionales de

ABOGADO Y NOTARIO

Guatemala, octubre 2012

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

DECANO:	Lic. Avidán Ortiz Orellana
VOCAL II:	Lic. Mario Ismael Aguilar Elizardi
VOCAL III:	Lic. Luis Fernando López Díaz
VOCAL IV:	Br. Modesto José Eduardo Salazar Dieguez
VOCAL V:	Br. Pablo José Calderón Gálvez
SECRETARIA:	Licda. Rosario Gil Pérez

TRIBUNAL QUE PRACTICÓ
EL EXAMEN TÉCNICO PROFESIONAL

Primera Fase:

Presidente:	Lic. Juan Ramón Peña Rivera
Vocal:	Lic. Emilio Gutiérrez Cambranez
Secretaria:	Licda. Rosa Orellana Arévalo

Segunda fase:

Presidente:	Lic. Ricardo Alvarado Sandoval
Vocal:	Licda. Eloisa Mazariegos Herrera
Secretario:	Lic. Jorge Eduardo Aviles Salazar

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. LESLY MADELIN CASTILLO LÓPEZ
ABOGADA Y NOTARIA
Colegiada: 9321
14 calle 6-12 zona 1 2do. nivel oficina 206 Edificio Valenzuela
Ciudad-Guatemala
Tel.: 22325185

Guatemala 16 de abril de 2012

Lic. Efraín Guzmán
Jefe de la Unidad de Asesoría de Tesis
Facultad de Ciencias Jurídicas y Sociales
Universidad de San Carlos de Guatemala
Su Despacho.

Estimado Licenciado Efraín Guzmán:

Hago de su conocimiento que en cumplimiento a la designación recaída sobre mi persona, según resolución proferida por la Unidad de Asesoría de Tesis a su digno cargo de fecha veintitrés de agosto del año dos mil once, del bachiller Axel Domingo Caz, asesoré el trabajo de tesis intitulado: **"LA IMPORTANCIA JURÍDICA DE IMPLEMENTAR MEDIDAS DE SEGURIDAD EN LOS MEDIOS DIGITALES PARA TRANSACCIONES ELECTRÓNICAS PARA EVITAR QUE TERCEROS LO UTILICEN PARA COMETER FRAUDE EN PERJUICIO DEL TARJETAHABIENTE".** Le doy a conocer que la tesis abarca:

1. Un contenido técnico y científico del tema que se investigó. Además, se consultó la legislación y doctrina relacionada, utilizando la terminología jurídica y redacción apropiada y se desarrollaron sucesivamente los diversos pasos del proceso investigativo.

2. El bachiller Axel Domingo Caz, en el análisis realizado a su tesis, señala claramente la importancia de implementar medidas de seguridad en los medios digitales para transacciones electrónicas.

3. Se utilizaron los métodos adecuados, siendo los mismos: método sintético, que se empleó para señalar la regulación legal de las transacciones electrónicas en el derecho mercantil; el método analítico, dio a conocer las características del fraude electrónico; el método inductivo, para aplicar la teoría al caso específico del comercio electrónico; y el método deductivo, estableció las características de la informática jurídica.

4. Los objetivos generales y específicos, fueron alcanzados al ser determinantes en señalar la importancia de implementar medidas de seguridad en los medios digitales para las transacciones electrónicas. También, la hipótesis se comprobó al indicar en la misma la importancia del análisis jurídico de no cometer ningún perjuicio en contra de los tarjetahabientes.

5. Se emplearon las siguientes técnicas de investigación: documental y de fichas bibliográficas, con las cuales se obtuvo de forma ordenada la bibliografía actual y relacionada con el tema investigado. Las conclusiones y recomendaciones se redactaron clara y sencillamente.

La tesis desarrollada por el sustentante cumple efectivamente 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, por lo que emito **DICTAMEN FAVORABLE,** para que pueda continuar con el trámite respectivo, para evaluarse posteriormente por el Tribunal Examinador en el Examen Público de Tesis, previo a optar al grado académico de Licenciado en Ciencias Jurídicas y Sociales.

Muy atentamente.

Licda. LESLY MADELIN CASTILLO LÓPEZ
ABOGADA Y NOTARIA
Colegiada: 9321
Asesora de Tesis

Licda. Lesly Madelin Castillo López
ABOGADA Y NOTARIA

FACULTAD DE CIENCIAS
JURÍDICAS Y SOCIALES
Ciudad Universitaria, zona 12
GUATEMALA, C.A.

UNIDAD ASESORÌA DE TESIS DE LA FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES. Guatemala, 01 de junio de 2012.

Atentamente, pase al LICENCIADO **CARLOS ENRIQUE PATZÁN POR,** para que proceda a revisar el trabajo de tesis del estudiante: **AXEL DOMINGO CAZ,** intitulado **"LA IMPORTANCIA JURÍDICA DE IMPLEMENTAR MEDIDAS DE SEGURIDAD EN LOS MEDIOS DIGITALES PARA TRANSACCIONES ELECTRÓNICAS PARA EVITAR QUE TERCEROS LO UTILICEN PARA COMETER FRAUDE EN PERJUICIO DEL TARJETAHABIENTE".**

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 establece: "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".

DR. CARLOS EBERTITO HERRERA RECINOS
JEFE DE LA UNIDAD DE ASESORÍA DE TESIS

cc.Unidad de Tesis
CEHR/iyrc

LIC. CARLOS ENRIQUE PATZÁN POR
ABOGADO Y NOTARIO
11 calle 3-10, zona 1, Ciudad-Guatemala
Tels: 22532778

Guatemala, 18 de junio de 2012

Doctor
Carlos Ebertito Herrera Recinos
Jefe de la Unidad de Asesoría de Tesis
Facultad de Ciencias Jurídicas y Sociales
Universidad de San Carlos de Guatemala
Su Despacho

Respetable Doctor Herrera:

Me honra informarle que en cumplimiento de la designación recaída sobre mi persona como revisor de tesis, del Bachiller AXEL DOMINGO CAZ, quien elaboró el trabajo de tesis intitulado: **"LA IMPORTANCIA JURÍDICA DE IMPLEMENTAR MEDIDAS DE SEGURIDAD EN LOS MEDIOS DIGITALES PARA TRANSACCIONES ELECTRÓNICAS PARA EVITAR QUE TERCEROS LO UTILICEN PARA COMETER FRAUDE EN PERJUICIO DEL TARJETAHABIENTE"**; le doy a conocer que la tesis abarca:

1. Un contenido científico y técnico del tema investigado, además se consultaron la doctrina y legislación adecuadas, utilizando una redacción y terminología jurídica acorde, clara y precisa, habiendo desarrollado sucesivamente los diversos pasos del proceso investigativo y dividiendo la misma en cinco capítulos.

2. El sustentante, en el análisis realizado señala la importancia del derecho de informático y de la protección jurídica de los datos y medios digitales.

3. Se emplearon los métodos apropiados, siendo los utilizados los siguientes: el método inductivo, se utilizó para determinar la importancia del derecho informático; el método deductivo, dio a conocer las características de la informática jurídica; el método analítico, estableció la titularidad del tarjetahabiente y el método sintético, estableció la regulación legal de las transacciones electrónicas.

4. La contribución científica del trabajo de tesis llevado a cabo, muestra con datos actuales que hay una ausencia de regulación específica para proteger a los tarjetahabientes de fraudes electrónicos cuando se realizan pagos en internet. También, la hipótesis se comprobó, al indicar la misma la importancia de regular la protección de los usuarios del comercio electrónico para que no sean estafados por medio de Internet y otros medios digitales.

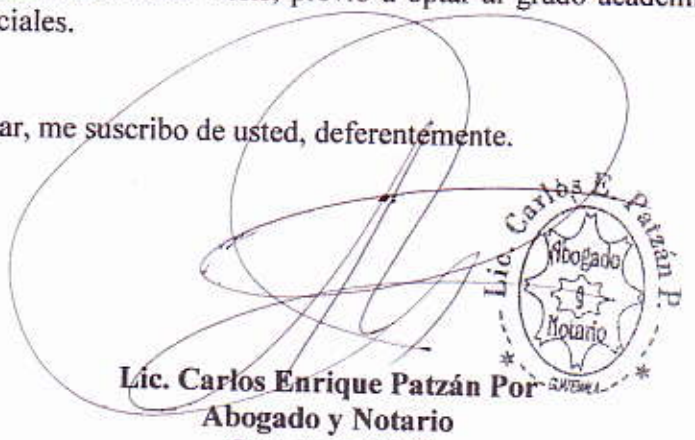
5. Las técnicas que se emplearon fueron la documental y de fichas bibliográficas, con las cuales se recolectó ordenadamente la bibliografía necesaria y actualizada relacionada con el derecho informático, el comercio electrónico y los medios digitales de pago.

6. La introducción, conclusiones y recomendaciones fueron redactadas en forma clara y sencilla; constituyendo supuestos válidos que dan a conocer la realidad nacional.

7. Al Bachiller Axel Domingo Caz le sugerí la necesidad de llevar a cabo algunas correcciones a los capítulos de su tesis, introducción y bibliografía, encontrándose conforme en su realización para una debida estructuración del tema investigado.

La tesis desarrollada por el sustentante cumple efectivamente 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, por lo que emito **DICTAMEN FAVORABLE,** para que pueda continuar con el trámite respectivo, para evaluarse posteriormente por el Tribunal Examinador en el Examen Público de Tesis, previo a optar al grado académico de Licenciado en Ciencias Jurídicas y Sociales.

Sin otro particular, me suscribo de usted, deferentemente.



Lic. Carlos Enrique Patzán Por
Abogado y Notario
Colegiado 5453
Revisor de Tesis

FACULTAD DE CIENCIAS
JURÍDICAS Y SOCIALES
Ciudad Universitaria, zona 12
GUATEMALA, C.A.

DECANATO DE LA FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES. Guatemala, 19 de septiembre de 2012.

Con vista en los dictámenes que anteceden, se autoriza la impresión del trabajo de tesis del estudiante AXEL DOMINGO CAZ, titulado LA IMPORTANCIA JURÍDICA DE IMPLEMENTAR MEDIDAS DE SEGURIDAD EN LOS MEDIOS DIGITALES PARA TRANSACCIONES ELECTRÓNICAS PARA EVITAR QUE TERCEROS LO UTILICEN PARA COMETER FRAUDE EN PERJUICIO DEL TARJETAHABIENTE. Articulos: 31, 33 y 34 del Normativo para la Elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Público.

BAMO/iyr.

Lic. Avidán Ortíz Orellana
DECANO

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

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

DEDICATORIA

A DIOS TODO PODEROSO: Ser supremo y dador de la vida, quien con su presencia en mis actos, me dio sabiduría, para alcanzar una meta más de las que me he trazado.

A MI MADRE: Manuela Caz. Con especial dedicación, a quien le debo lo que soy; que el triunfo que hoy obtengo sea una pequeña recompensa a sus esfuerzos de ayer, y aspiraciones de hoy.

A MI ESPOSA: Miriam Liceht Alvarado Molina. Por estar siempre a mi lado, compartiendo mis alegrías, triunfos y circunstancias adversas, instándome a seguir adelante.

A MIS HERMANAS Y SOBRINOS María Isabel, Carmelina, Aracelly, Kevin, Yoselin, y Richard. Por confiar siempre en mi persona, que mi triunfo obtenido, les sirva de ejemplo.

A MI MADRINA: Letti Taracena Alva. Con especial cariño, por su constante apoyo moral.

A MIS SUEGROS: Ruvinda Molina y Benito Alvarado. Con especial cariño, por confiar siempre en mi persona.

A MIS AMIGOS: Licda. Lesly Castillo, Licda. Mildred Pérez, Lic. Carlos Patzán, Lic. Jorge Paredes, Lic. Luis Garcia, Lic. Marlon Batres, Gilberto Pernilla, Julio Debroy, Agustin Cabrera, Minicio Silva, Alicia Hernández, Luis Morales y demás amigos. Por su constante apoyo moral.

A: La gloriosa Facultad de Ciencias Jurídicas y Sociales de la Universidad de San Carlos de Guatemala. Con mucho agradecimiento, por formarme académicamente.

ÍNDICE

CAPÍTULO V

Pág.

INTRODUCCIÓN

Ante la modernización de las actividades mercantiles, se presentan opciones de compra-venta que en el mercado guatemalteco no existían hace diez años. Esto ha permitido el surgimiento de formas electrónicas de pago, las cuales se manifiestan a través de tarjetas de crédito o debito, que el usuario puede utilizar con el fin de agilizar la adquisición de bienes; sin embargo, esta digitalización de las transacciones también generó el surgimiento de nuevas formas de fraude, ante lo cual se consideró importante analizar las medidas de seguridad utilizadas en las transacciones electrónicas, que eviten que terceros los utilicen para cometer fraude en perjuicio del tarjetahabiente.

La hipótesis que se estudió y comprobó es que los oferentes de los medios digitales de pago han implementado mecanismos técnicos para reducir los riesgos de estafa para los usuarios; sin embargo la legislación guatemalteca todavía no ha establecido formas jurídico-legales para enfrentar a los defraudadores en este tipo de actividades.

Los objetivos se lograron al determinar la importancia de la informática y el derecho informático en Guatemala; al describir el crecimiento del comercio electrónico; y la evolución de los medios digitales para transacciones electrónicas; así como las características del fraude electrónico.

Los métodos utilizados fueron el deductivo, para fundamentar doctrinariamente el trabajo de tesis; el inductivo, para aplicar la teoría al caso específico del comercio electrónico; el analítico, con el cual se explican las características del fraude electrónico y con el sintético

se abordan los aspectos centrales de este ilícito en las transacciones digitales. La técnica utilizada fue la bibliográfica con la cual se clasificaron los libros vinculados con la doctrina del comercio electrónico, la informática y el derecho informático.

Luego de procesar la información obtenida, se redactó el informe final de tesis, el cual consta de cinco capítulos: El primero se orientó hacia la explicación de la informática y el derecho informático; el segundo, explica el comercio electrónico y su importancia; en el tercero, se explican los elementos de los medios digitales para las transacciones electrónicas; el cuarto, sirvió para caracterizar el fraude electrónico; mientras que el quinto, se dirigió a fundamentar los elementos que deben implementarse como medidas de seguridad en los medios digitales para transacciones electrónicas.

Con la presente investigación se considera haber llevado a cabo un adecuado aporte a la configuración de los elementos que deben informar una legislación orientada hacia la protección legal de los tarjetahabientes y su relación con el comercio electrónico.

CAPÍTULO I

1. Informática y derecho informático

La informática es una ciencia que estudia el procesamiento lógico y automático de la información; la misma ha sido empleada en todas las actividades del ser humano en busca de una mejor eficiencia y de un trabajo más rápido.

Es un hecho que la computadora en particular y la informática en general, han invadido sectores muy amplios del quehacer social, al grado de considerársele imprescindible, pues no es raro que se tomen decisiones o se orienten ciertas actividades cotidianas en función estricta del apoyo tecnológico y logístico que los avances técnicos proporcionan.

"Se parte del hecho cierto e innegable de que en el presente, se encuentran computadoras, equipo y material informático prácticamente en cualquier parte. En efecto, se hallan en bancos, hospitales, despachos contables, aulas, escuelas, universidades, instituciones carcelarias y correccionales, vehículos de cualquier clase (aviones, barcos, naves espaciales), supermercados, consultorios privados, tribunales, bibliotecas, cuarteles militares, hogares, bufetes jurídicos, empresas públicas y privadas de la más diversa naturaleza, aeropuertos, notarías, laboratorios, hoteles, corporaciones policiacas, registros públicos y privados, así como agencias de investigación penal. Además, basta revisar la prensa cualquier día para percatarse de la avalancha comercial que en el campo informático existe en esta época y comprobar con ello que, en la sociedad actual, tal

informática desempeña un papel muy destacado y preponderante".[1]

De igual manera, los sistemas inteligentes, llamados también expertos, así como muchos otros géneros de herramientas tecnológicas, en este caso, de carácter informático y tele-informático, son de uso común; forman parte del instrumental cultural de la sociedad de este momento y, a la fecha, impactan fuertemente en el quehacer social; y el derecho, como es obvio, no es ni debe ser la excepción a ello.

Palabras tales como realidad virtual, software, internet, módem, computadora, dinero electrónico, CD-rom, firma digital, fax, entre otras muchas, forman ya parte del léxico cotidiano y son de uso corriente; por lo que los abogados no pueden ni deben permanecer al margen de ello, pues ignorar la vertiente jurídica del fenómeno informático es como cerrar los ojos a la realidad, con el consecuente olvido de que el derecho es para la vida.

"El término informática fue creado en Francia, a mediados de la década de los sesenta (informatique, de infor-mation-auto-matique), con el objeto de designar las ciencias y técnicas de la comunicación que intervienen en la recopilación y utilización de datos a fin de elaborar decisiones, extendiéndose de ahí y a partir de esa época, a todo el mundo. Información automática, procesada en medios electrónicos; sus elementos son: la información, su materia prima, voz e imagen; el hardware, el equipo; el software del procesamiento y las telecomunicaciones, sus prolongaciones; sus funciones son: procesar a alta velocidad, gran cantidad de información y almacenarla en espacio mínimo (disco duro, flexible y óptico); transmitirla casi instantáneamente, a grandes distancias y posibilitar

[1] Martino, Antonio. **Sistema expertos legales**. Pág. 35

el facsímil o la impresión; agilizar la recuperación de los datos en cualquier futuro inmediato o diferida; reconocer voces e imágenes personales. Cada día incorpora mayor expertización en sus sistemas, hasta llegar a la inteligencia artificial (en la transición de la cuarta a la quinta generación). Aprovecha la microminiaturización progresiva (chips, microcircuitos impresos, fibras ópticas) para generar espacio. Se vale de la aceleración progresiva para ganar tiempo; obtiene su propio abaratamiento para ahorrar esfuerzos (por ejemplo, sustituye a la dactilografía con el escaneado de textos e imágenes), todo ello con el fin de disponer dónde, cuándo y cómo se requiera, de una información útil, veraz y oportuna".[2]

Esto implica que el término informática o información automática, encierra el tratamiento racional que hace una mayor eficacia y rapidez en la elaboración y transmisión de información, superando grandes barreras de tiempo y distancia, en condiciones hasta hace poco tiempo inimaginables; por lo que la informática, entonces, es la ciencia y técnica que estudia, o se refiere al diseño y utilización de equipos, sistemas y procedimientos para obtener, recuperar, almacenar, transmitir y procesar información, buscando entre otras cosas, el control sobre la información por parte del operador.

"La informática es la ciencia del tratamiento racional, particularmente por máquinas automáticas, de la información considerada como el soporte de conocimientos humanos y de comunicación en los aspectos técnicos, económicos y social. Conjunto de disciplinas científicas y técnicas específicamente aplicables al tratamiento de datos efectuado por medios automáticos".[3]

---

[2] Bielsa, Rafael. **Informática y derecho: aportes de doctrina internacional**. Pág. 135
[3] **Ibid.**

Se puede sintetizar, en pocas palabras a la informática, como el conjunto de técnicas que posibilitan la manipulación rápida o automática de información; porque se está hablando en este terreno de la automatización de la información.

1.1. La automatización en general y su irrupción en el universo jurídico

El fenómeno de la automatización irrumpe fundamentalmente a partir del mundo industrial de la producción en masa del siglo XX; arreciando dicho fenómeno, a no dudarlo, en la llamada era pos-industrial.

"Desde un punto de vista general, puede afirmarse que la automatización consiste en que los órganos humanos del esfuerzo, de atención, de observación y de memoria son sustituidos por órganos tecnológicos. Con la automatización funcionan instalaciones a base de procedimientos que permiten repetir las operaciones, de donde surge la importancia de la autorregulación de todo mecanismo de producción. Lo que supone, además de una serie de perfeccionamientos técnicos, un sistema de producción que combina principios bien establecidos y diversas teorías recientes que se refieren a la posibilidad de registrar informaciones y de comunicarlas a las máquinas por medio de órganos-memoria. Nacieron estas teorías en la Segunda Guerra Mundial, cuando era sumamente necesario poner a punto una serie de dispositivos automáticos y autorreguladores para los aviones guiados por radar".[4]

La aplicación de la electrónica ha influido mucho en la difusión de la automatización,

[4] Ibid.

porque los progresos prodigiosos de esta ciencia han invadido todos los dominios, procurándole nuevas formas de transmisión, de memoria; los cuales por su velocidad, poder y capacidad, tienen una eficacia que supera millones de veces estas cualidades.

La contribución de la electrónica a la automatización ensancha el empleo de los mandos autómatas y permite el tratamiento rápido, preciso y automático de las informaciones, que es en lo que consiste precisamente la informática; la cual se ha impuesto en todas las esferas de las relaciones humanas, porque en el presente la tecnología de la información y la comunicación han permitido la digitalización de todos los procesos de relacionamiento humano, haciendo fáciles las tareas cotidianas.

1.2. La informática jurídica

En el campo del derecho, también se ha producido la automatización porque se han ido desarrollando una serie de técnicas para la ordenación electrónica de datos y procedimientos jurídicos, ya cristalizada bajo el nombre de informática jurídica.

"La informática jurídica estudia el tratamiento automatizado de las fuentes del conocimiento jurídico a través de los sistemas de documentación legislativa, jurisprudencial y doctrinal, conocida como informática jurídica documental; las fuentes de producción jurídica, a través de la elaboración informática de los factores lógico-formales que concurren en el proceso legislativo y en la decisión judicial o informática jurídica decisional; así como los procesos de organización de la infraestructura o medios instrumentales con los que se gestiona el derecho, conocida también como informática

jurídica de gestión".[5]

Lo citado significa que son las aplicaciones de programas de computador para satisfacer necesidades jurídicas las primeras en nacer en el tiempo, motivadas por una confluencia de factores tecnológicos. Transcurrirían, en cambio, bastantes años aún para que viniera a darse el movimiento inverso, esto es que el derecho reaccionara ofreciendo su marco regulador a varios fenómenos propios de la diseminación de la informática en la sociedad. De igual manera, la propia informática jurídica durante mucho tiempo no fue sino una aproximación técnica a la espera de los futuros desenvolvimientos tecnológicos que le permitirían luego operar en forma empírica.

"Lee Loevinger fue el primero que imaginó el uso de las computadoras para coadyuvar en la resolución de una problemática jurídica; la violación o no del régimen antimonopolio en el sistema jurídico norteamericano. Corría el año 1949 cuando este manager al frente de la oficina encargada de dichos controles acuña el término jurimetría, a propósito de poder llegar a medir si ello fuera posible la conducta de los jueces dentro del sistema jurídico como el anglosajón, en el cual el descubrimiento del precedente judicial pertinente dentro de una masa creciente de los mismos ha sido siempre una concreta necesidad para el funcionamiento del sistema jurídico. Pero habría que esperar el año 1963 para que se produjera la primera impostación teórica de lo que correspondería incluir dentro de esta llamada jurimetría, ancestro de nuestra actual informática jurídica. Fue en esa fecha que Hans Baade, al prologar una obra colectiva sobre jurimetría y definiendo a ésta como el análisis científico de los problemas jurídicos, señala tres áreas de estudios y aplicaciones:

[5] Falcon, Enrique. **¿Qué es la informática jurídica?: del ábaco al derecho informático.** Pág. 119.

Primera, la memorización y recuperación de datos contenidos en soporte informático; segunda, el análisis conductista de las decisiones judiciales mediante revelamientos estadísticos y cálculos probabilísticos y tercera, la aplicación de la lógica simbólica a los fallos y normas jurídicas en general".[6]

Como se puede apreciar, esta primera fase tiene lugar dentro del sistema jurídico del derecho estadounidense, en un ambiente cultural y unas necesidades de ejercicio y práctica del derecho; que llevó a descubrir ciertas utilidades del computador para objetivos fundamentalmente de tipo documental y provisional, en cuanto a la conducta seguida por los jueces ante similares casos.

La necesidad del surgimiento de la informática jurídica se encuentra en el crecimiento de las fuentes de información en todos sus géneros, lo cual se volvió incontrolable, cada vez más imposible de ser conocida al continuar utilizándose métodos manuales. La computadora, con su gran capacidad de almacenamiento de datos y su potentosa velocidad de clasificación de los mismos a través de innumerables canales de búsqueda y recuperación, comienza ya en esa época a vislumbrarse en todo su potencial por algunas personas vinculadas al mundo jurídico.

"Hacia fines de los años sesenta, la difusión de aplicaciones informáticas en la sociedad resulta ya suficientemente representativa como para denunciar implicaciones sociales y jurídicas. Emerge, así la llamada informática jurídica, con nombres pioneros como los de Bigelow y Colin Tapper. Se revelan como primeras preocupaciones la acumulación y uso

[6] **Ibid.**

indebido de los llamados datos personales, con el posible conflicto de este hecho y el derecho de intimidad o privacidad. También los contratos de equipamiento informático y la protección a los autores de los programas de computación en cuanto a los derechos morales y de explotación de su obra, aparecen entre estas primeras inquietudes desarrolladas y ampliadas rápidamente en los sucesivos años. En la misma época se dedican artículos al tema de la automatización de la gestión de los estudios profesionales y la actividad procesal de la justicia, con lo cual nace la llamada informática jurídica de gestión".[7]

Estos elementos permiten ver que la informática jurídica tiene doble objeto. Por un lado, las aplicaciones de la computadora al derecho y por otro lado, los problemas jurídicos derivados del impacto de estas tecnologías en la sociedad y su consecuente reglamentación legal; en donde la informática jurídica es una materia inequívocamente jurídica, conformada por el sector normativo de los sistemas jurídicos contemporáneos integrado por el conjunto de disposiciones dirigido a la regulación de las nuevas tecnologías de la información y la comunicación; es decir, la informática y la telemática.

"Durante los primeros tiempos, las aplicaciones en el ámbito del derecho en materia informática, estuvieron limitadas a la utilización de bancos de datos para cargar, clasificar y procesar información jurídica de relevancia, sea legislación, jurisprudencia o doctrina. Con el correr del tiempo, comenzaron a desarrollarse otras clases de aplicaciones, destinadas a realizar mediante el computador diversas tareas de orden repetitivo, tanto en el área registral como en el judicial y en el profesional. El continuo desarrollo tecnológico produjo

[7] **Ibid.** Pág. 120.

hechos insospechados, tales como la posibilidad de utilizar computadoras para adoptar decisiones en relación a ciertas cuestiones jurídicas, mediante el uso de sistemas expertos y seudoexpertos".[8]

Se entiende entonces, que la informática jurídica tiene por finalidad almacenar, ordenar, procesar y entregar todos los datos jurídicos necesarios para documentar o proponer la solución al problema de que se trate, mediante el estudio del tratamiento automatizado de las fuentes de conocimiento jurídico y de los medios instrumentales con que se gestiona el derecho.

1.3. El documento electrónico y el documento informático

Cuando en la informática en general y en la jurídica en particular, se hace referencia a documentos electrónicos se refiere a los documentos generados por medios electrónicos, o que son transmitidos o transcritos, respecto a su contenido, por medios electrónicos. Entre esos documentos también figuran los informáticos, no porque se considere a la informática como una parte de la electrónica, sino porque la informática utiliza la electrónica en la generación, transmisión o transcripción del documento.

De esta forma, se encuentran documentos generados o transmitidos por medios electrónicos y que no tienen relación alguna con la informática, como puede ser, por ejemplo, el consecuente de un mensaje transmitido por fax, donde aquélla no ha intervenido.

[8] **Ibid.**

También se debe considerar que el documento electrónico en el que, además del componente informático, se haya utilizado un medio de comunicación entre ordenadores, con el que al unir informática y comunicaciones -fruto de ello es la telemática- se habla de documentos generados o transmitidos telemáticamente. Luego, en el sentido ya expuesto, se dice que hay documentos generados o transmitidos por medios electrónicos, documentos generados por medios informáticos o de documentos generados por medios telemáticos; a los cuales en su conjunto, por razones de simplificación, se les denomina documentos electrónicos a los primeros, informáticos a los segundos y telemáticos a los últimos. Serán documentos electrónicos, documentos informáticos o documentos telemáticos.

"Se hace referencia a documentos informáticos y/o telemáticos uniendo ambos bajo la característica común del tratamiento de la información propia de la informática. Para ello, se diferencia por un lado el documento que encuentra como destino físico el soporte papel, por ser fácil de encuadrar dentro de las teorías aceptadas en los ordenamientos jurídicos de nuestro ámbito; de otro lado, el documento que encuentra como destino un soporte de los comúnmente utilizados en informática, distinto del soporte papel, como puede ser el caso de un diskette, compact disk, cinta magnética o cualquier otro soporte adecuado para ello; y, por último, el documento que encontrando como soporte final uno de los que hemos denominado informático, ha sido enviado mediante comunicaciones por una red telemática, y por tanto, ha sufrido un viaje a través de la red. De esta forma estudiamos tres posibles aspectos de los documentos informáticos y/o telemáticos: un primer aspecto en el que consideramos el soporte de información papel, generado a través de medios informáticos; esto es, el listado impreso de la información que se encuentra en un soporte

informático o que ha sido generada a través de medios informáticos; lo que vamos a denominar, siguiendo una nomenclatura extendida, un printout, y que es un documento que la evolución de la tecnología y la necesidad de manejo de grandes cantidades da datos, ha hecho que sea considerado normal y aceptado por todos al ratificar su contenido con símbolos tradicionales que les convierte en originales como, por ejemplo la firma. Un segundo aspecto en el que consideramos el documento como aquél que se encuentra en un soporte de información electrónica creado por datos almacenados en la memoria de un ordenador, lo que vamos a denominar siguiendo la misma nomenclatura un input; este documento no tiene porque ser forzosamente un auténtico input; en el sentido de entrada hacia el ordenador, ya que puede ocurrir que sea producto de un proceso informático que ha dado como resultado su contenido y este contenido es almacenado en un soporte de los que hemos llamado informáticos, este documento puede ser transcrito sin dificultad a un soporte papel, convirtiéndose en un printout. Y un tercer aspecto en una modalidad muy extendida y aceptada en los últimos tiempos considerado como soporte de información electrónico, formado mediante el intercambio de mensajes, con una estructura determinada, utilizando unas normas de intercambio informáticos".[9]

Estos tres tipos de documentos, dos de ellos en soporte informático y en soporte papel el otro, presentan determinadas características y distintas particularidades que hacen se les deba analizar por separado en dos clases; según que el soporte final sea el papel o no.

Respecto a los documentos que se encuentran en soporte papel resultado de la salida impresa del contenido de un soporte informático, parecen no plantear demasiados

[9] Davara Rodríguez, Miguel Angel. **El documento electrónico.** Pág. 17.

problemas ya que es, en definitiva, este listado impreso el que va a ser considerado como documento y su contenido se valorará independiente del que figure en el soporte informático, siendo el del papel el que va a ser tenido en cuenta, aunque exista una total identidad.

Los otros tipos de documentos en soporte informático ofrecen en principio más dudas, ya que, aunque se llegue a la conclusión de su aceptación, problemas de originalidad del documento o de posibilidad de modificación o transformación de su contenido, debido al procesamiento al que pueden ser sometidos en el momento de su exteriorización en lenguaje natural por un procedimiento informático; hacen que se extremen las seguridades y no se pueda en una primera interpretación hablar genéricamente de su validez y originalidad.

Ello es debido a que los documentos que se encuentran en un soporte informático necesitan para poder ser visualizados e interpretados en lenguaje natural de un proceso mediante un programa, con un procedimiento lógico, que convierta la expresión en codificación informática, a la misma expresión en lenguaje natural y la representen en un soporte que pueda ser visualizado directamente por el nombre. Esto conlleva, en aras de una seguridad física, de procedimiento lógico y, evidentemente jurídica, a que el método de interpretación para poder comprobar visualmente, ya sea en una pantalla de computadora o en el soporte papel de la impresión, el contenido del documento esté sometido a unas garantías que aseguren su autenticidad.

Este es el único problema y la única objeción que se les pone, siendo, por otro lado, muy

sencillo garantizar estos procedimientos por medios tecnológicos; de forma que ofrezcan una seguridad de coincidencia con el contenido original y hagan fiable el documento informático.

1.4. Derecho Informático

No cabe la menor duda de que el derecho informático es una materia nueva en la ciencia jurídica; la cual está conformada por el sector normativo de los sistemas jurídicos contemporáneos integrados por el conjunto de disposiciones dirigido a la regulación de las nuevas tecnologías de la información y la documentación; es decir, la informática y la telemática.

Asimismo, integran el derecho informático las sentencias de los tribunales sobre materias informáticas y las proposiciones normativas; es decir, los razonamientos de los teóricos del derecho que tienen por objeto analizar, interpretar, exponer, sistematizar o criticar el sector normativo que disciplina la informática y la telemática.

El derecho informático constituye una ciencia autónoma del derecho que abarca el estudio de las normas, jurisprudencia y doctrinas relativas al control y regulación de la informática en su expansión y desarrollo; así como la aplicación idónea de los instrumentos informáticos.

"El derecho informático es la aplicación del derecho a la transformación permitiendo que se adopten o creen soluciones jurídicas a los problemas que surgen en torno al fenómeno

informático".[10]

El derecho informático es la rama del derecho encargada de estudiar los cambios, fenómenos y paradigmas que se producen actualmente en las instituciones jurídicas debido a la intromisión de las tecnologías de la información y comunicación en la sociedad; afectando las estructuras jurídico políticas, económicas inclusive interpersonales. Asimismo, aborda el estudio de las tecnologías de la información y comunicación desde dos ejes; el primero de ellos estudia la tecnología como objeto del derecho, mientras que el segundo estudia la tecnología como instrumento del derecho.

La tecnología como objeto del derecho, es estudiada a partir de los cambios que se han generado en todas las instituciones jurídicas, generando nuevos lineamientos y principios para estas tendencias modernas, toda vez que el derecho tradicional se queda corto al tratar de abarcar una problemática actual. A partir de ello estudia al comercio electrónico, los derechos de autor en internet, los nombres de dominio, la privacidad, el teletrabajo, los delitos informáticos, los contratos informáticos y telemáticos, aspectos tributarios en la red, los aspectos legales de internet, del software y de la sociedad de la información.

Por otro lado se encuentra la tecnología como instrumento del derecho, en donde éste se vale de las tecnologías para desarrollar su actividad que le permite optimizar las tareas que se le han encargado; por ejemplo en casos como la informática jurídica de gestión, parlamentaria, ofimática jurídica, sistemas expertos jurídicos y bases de datos.

[10] Nuñez Ponce. Julio. **Derecho informátco.** Pág. 22

"El derecho informático es el sector normativo de los sistemas, dirigido a la regulación de las nuevas tecnologías de la información y la comunicación, es decir, la informática y la telemática. Asimismo integran el derecho informático las proposiciones normativas, es decir, los razonamientos de los teóricos del derecho que tienen por objeto analizar, interpretar, exponer, sistematizar o criticar el sector normativo que disciplina la informática y la telemática. Las fuentes y estructura temática del derecho informático afectan las ramas tradicionales del derecho". [11]

Asimismo, resulta objeto del derecho informático el problema de la regulación del flujo internacional de datos informatizados, la libertad informática o defensa de las libertades frente a eventuales agresiones perpetradas por la tecnología de la información y la comunicación o los delitos informáticos con carácter internacional.

"De igual manera, son objeto de estudio y regulación los contratos informáticos, que pueden afectar lo mismo al hardware que al software, dando lugar a una rica tipología de los negocios en la que pueden distinguirse contratos de compraventa, alquiler, leasing, copropiedad, multicontratos de compraventa, mantenimiento y servicios; como los distintos sistemas para la protección jurídica de los objetos tradicionales de los derechos civiles y mercantiles". [12]

Ese mismo carácter interdisciplinario o transversal, que distingue al derecho informático, ha suscitado un debate teórico sobre si se trata de un sector de normas dispersas pertenecientes a diferentes disciplinas jurídicas o constituye un conjunto unitario de

[11] **Ibid.**
[12] Ibid. Pág. 24.

normas fuentes, dirigidas a regular un objeto bien delimitado; que se enfoca desde una metodología propia, en cuyo supuesto entraría una disciplina jurídica autónoma, lo cual predomina en la actualidad.

"*El derecho informático, como una nueva rama del conocimiento jurídico*, es una disciplina en continuo desarrollo, teniendo en su haber (al menos hasta la fecha) incipientes antecedentes a nivel histórico. Las primeras manifestaciones interdisciplinarias se daban en los términos instrumentales de las aplicaciones informáticas respecto al derecho, lo cual se desarrolla extra-conceptualmente en la década de los cincuenta, a diferencia del estudio de las implicaciones jurídicas motivadas por la informática que comienza a desarrollarse en la década de los sesenta".[13]

Esta nueva disciplina jurídica tiene métodos e instituciones propias que surgen de un fenómeno que tiene implicaciones globales y que por tanto; permite tener bases doctrinales y principios similares con las peculiaridades propias de cada ordenamiento jurídico.

Esta realidad jurídica se orienta hacia el análisis de las implicaciones que recaen sobre sus más diversos ámbitos. No existe espacio que no haya debido avocarse a problemas o interrogantes originados por la sociedad de la información: teletrabajo, manipulación y venta de datos sensibles almacenados digitalmente, tributación de operaciones comerciales originadas en lugares desconocidos, nuevos delitos penales como el hacking, craking, sniffers, ciberpunk, estafas virtuales o el gobierno electrónico, son algunos de los

[13] **Ibid.** Pág. 26.

temas que cruzan las construcciones legales formuladas para una realidad analógica y de contactos en persona.

El derecho de la contratación no es ajeno a la problemática. El acuerdo de voluntades sobre intereses económicos, instrumentos del intercambio de bienes y servicios, se vehiculiza a través de las redes en forma exponencial. Los diversos actores involucrados, gobiernos nacionales y comunitarios, organizaciones gubernamentales y no gubernamentales, asociaciones profesionales, doctrinarios, han propuesto soluciones y herramientas para superar las barreras culturales y jurídicas de las regulaciones delineadas en los siglos XIX y XX para el comercio. El concepto mismo de contrato electrónico, los principios que rigen al comercio electrónico, los elementos objetivos y subjetivos intervinientes, la representación electrónica, el momento y lugar de perfección del contrato, el cumplimiento electrónico de las obligaciones contractuales, etc.

"El contrato electrónico es una manifestación más del intercambio de datos a través de las redes. Las personas pueden comunicarse electrónicamente con fines de trabar o cultivar amistades, de buscar información en alguna de las múltiples bases de datos existentes en la red, de informarse en los periódicos digitales, o de comerciar. El comercio realizado a través de medios electrónicos es denominado ecommerce, caracterizado por la transnacionalización e impersonalización. Se le denomina B2B, si es entablado entre empresas, B2C, si la relación se traba entre empresas y consumidores, y C2C, si lo es entre consumidores".[14]

[14] Márquez, José Fernando. **Elementos de la contratación electrónica.** Pág. 9.

El intercambio de datos o mensajes electrónicos, vehículos de las declaraciones de voluntad u oferta y aceptación que concluirán el contrato, puede realizarse en redes cerradas o en redes abiertas.

"El contrato en redes cerradas (acuerdos conocidos como EDI –electronic data interchange-) trae al derecho menos problemas, pues, por lo general, está precedido por un acuerdo de intercambio de datos, en el cual se determinan las reglas técnicas y jurídicas que harán vinculantes a las declaraciones. La contratación en redes abiertas (como la internet), por el contrario, presenta numerosos aspectos a resolver. Los principales: asegurar la identidad de las partes autoras de los mensajes, la integridad del mensaje (su no adulteración) y la emisión y recepción del mensaje (el no repudio)".[15]

La firma digital en los mensajes de datos tiende a asegurar la identidad del autor y la integridad del mensaje, a través de técnicas de encriptación. Se persigue el no repudio del envío o recepción por medio del acuse de recibo y la confirmación del envío. Cuando una de las partes contratantes envía un mensaje electrónico conteniendo una oferta necesita saber si el mensaje fue recibido, a fin de conducir su conducta en consecuencia. Por ello es imprescindible crear medios que otorguen certeza de la recepción del mensaje, para dotar a la contratación electrónica de seguridad. Ello se intenta obtener a través de la imposición al receptor del mensaje (ofertado) del envío de un mensaje que sirva de aviso de recepción (acuse de recibo) del mensaje original.

Este capítulo se orientó a explicar la informática y el derecho informático, lo cual resulta

[15] **Ibid.**

fundamental en la realidad virtual presente, pues en las actividades diarias de la mayoría de guatemaltecos de las áreas urbanas existe una profunda vinculación con las tecnologías de la información y la comunicación, que debiera encontrarse mejor regulada en la legislación guatemalteca, puesto que la misma se ha convertido en un elemento central de la cultura del país, de lo cual no debe estar ajeno el derecho para que establezca normas legales de uso y aplicación con lo cual se garantiza seguridad jurídica a las personas en las actividades donde utilicen los procedimientos digitalizados.

CAPÍTULO II

2. El comercio electrónico

El significado del comercio electrónico ha cambiado a lo largo del tiempo, porque originalmente significaba la facilitación de transacciones comerciales electrónicamente.

"El comercio electrónico comenzó a ser posible a partir de que se pudo hacer uso de tecnología como la Electronic Data Interchange (EDI, presentada a finales de los años 70) para enviar electrónicamente documentos como pedidos de compra o facturas. Más tarde pasó a incluir actividades más precisamente denominadas comercio en la red –la compra de bienes y servicios a través de la World Wide Web vía servidores seguros (HTTPS, un protocolo de servidor especial que encripta la realización confidencial de pedidos para la protección de los consumidores y los datos de la organización) con tarjetas de compra electrónica y con servicios de pago electrónico como autorizaciones para tarjeta de crédito. En 1995 los países integrantes del G7/G8 crearon la iniciativa Un Mercado Global para PYMES (en inglés), con el propósito de acelerar el uso del comercio electrónico entre las empresas de todo el mundo".[16]

"Algunos expertos opinan que en cierta forma, el comercio electrónico comenzó antes de internet, mediante transacciones comerciales por télex (teléfono y fax), pero el desarrollo de la web global motivó que alcanzara mayor auge, por su masividad y rapidez de operación. Su acepción más general es acercar el comprador al fabricante por medios

[16] Acedo Quezada, Octavio. **Temas y problemas que la informática ocasiona en la formación del consentimiento contractual**. Pág. 103.

electrónicos, lo cual implica eliminación de intermediarios, reducción de costos y una filosofía diferente en la forma de comprar y vender, y lo que es más importante, de obtener información para esas gestiones".[17]

Esto significa que el comercio electrónico consiste principalmente en la distribución, compra, venta, mercadeo y suministro de información complementaria para productos o servicios a través de redes informáticas como internet u otras redes informáticas; por lo que puede ser cualquier forma de transacción comercial en la cual las partes involucradas interactúan de manera electrónica y no de la manera tradicional por medio de intercambios físicos o trato físico directo.

"El comercio electrónico es cualquier actividad de intercambio comercial en la que las órdenes de compra-venta y pagos se realizan a través de un medio telemático, los cuales incluyen servicios financieros y bancarios suministrados por internet. El comercio electrónico es la venta a distancia aprovechando las grandes ventajas que proporcionan las nuevas tecnologías de la información, como la ampliación de la oferta, la interactividad y la inmediatez de la compra, con la particularidad que se puede comprar y vender a quien se quiera, donde y cuando se quiera. Es toda forma de transacción comercial o intercambio de información, mediante el uso de nueva tecnología de comunicación entre empresas, consumidores y administración pública".[18]

Como se puede apreciar, por comercio electrónico se entiende la compra y venta de productos y servicios a través de un medio electrónico o red informático; por lo que

[17] **Ibid.**
[18] Ibid. Pág. 106.

también es conocido como ecommerce (electronic commerce, en inglés); consiste en la compra y venta de productos o de servicios a través de medios electrónicos, tales como internet y otras redes informáticas.

Originalmente el término se aplicaba a la realización de transacciones mediante medios electrónicos tales como el intercambio de datos; sin embargo, con el advenimiento de la internet y las paginas web, a mediados de los años noventa comenzó a referirse principalmente a la venta de bienes y servicios a través de internet; usando como forma de pago medios electrónicos, tales como las tarjetas de crédito.

La cantidad de comercio llevada a cabo electrónicamente, ha crecido extraordinariamente debido a la propagación del internet. Una gran variedad del comercio se realiza de esta manera, estimulando la creación y utilización de innovaciones como la transferencia de fondos electrónica, la administración de cadenas de suministros, el mercadeo en internet, el procesamiento de transacciones en línea, el intercambio de datos, los sistemas de administración del inventario y los sistemas automatizados de recolección de datos.

La mayor parte del comercio electrónico es la compra y venta de productos o servicios entre personas y empresas; sin embargo, un porcentaje considerable del comercio electrónico consiste en la adquisición de artículos virtuales, tales como el acceso al contenido de un sitio web.

"El comercio electrónico realizado entre empresas es llamado en inglés Business-to-business o B2B, puede estar abierto a cualquiera que esté interesado (como el intercambio

de mercancías o materias primas), o estar limitado a participantes específicos precalificados (mercado electrónico privado), porque el comercio electrónico es la forma que adquieren los actos de comercio gracias a la convergencia de las diversas tecnologías de información existentes. Esta relación comercial puede tomar una forma completamente digital, en la medida en que el bien o servicio ofrecido-adquirido y el medio de pago tengan un soporte completamente electrónico, o simplemente dar lugar a un desplazamiento físico de mercaderías y dinero".[19]

Dentro de las condiciones que han favorecido el auge durante los últimos años del comercio electrónico; se encuentran las constantes presiones a las que se ven sometidas las empresas para reducir sus costos y mantenerse vigentes en un ambiente competitivo; ya que éste permite reducir los costos en lo referente a las transacciones con los proveedores, publicidad, intercambio de información y servicio a los clientes.

2.1. Características

En el comercio tradicional, un mercado es un lugar físico al que se acude para comprar o vender; mientras que en el comercio electrónico se puede hacer desde cualquier parte del mundo, a cualquier hora; eso determina que el mercado potencial para las empresas en este negocio es toda la población mundial con acceso a internet; para lo cual desaparecen las barreras nacionales y regionales, aunque todavía sigue siendo necesario llevar los productos comprados vía electrónica de alguna manera al hogar del comprador.

[19] ALADI – Secretaría General. **Situación actual y perspectivas del comercio electrónico en la región.** Pág. 28.

Los estándares de internet son mundiales, lo cual disminuye los costos de entrada al mercado para las empresas y también reduce el esfuerzo de búsqueda por parte de los consumidores; presentándose la facilidad de comparar precios, descripciones de productos, proveedores, plazos de entrega; aunque esto es algo que todavía puede automatizarse muchísimo más, al extremo que en un par de décadas todas las empresas y todos los consumidores estarán presentes en la autopista digital.

"En la web, es posible añadir color, audio, texto, imágenes, es decir, más riqueza a los documentos a un costo prácticamente nulo, siendo ésta una de las principales ventajas cualitativas del medio digital del resto de medios. A diferencia de la mayor parte de medios tradicionales, el comercio electrónico permite una comunicación en ambos sentidos entre el comerciante y el consumidor, asimismo, permite la movilidad de una gran cantidad y calidad de la información disponible a todos los participantes del mercado. En el comercio electrónico que se incrementa drásticamente, hay aumento de la competencia real, efectiva, lo cual permite personalizar la información al consumidor, mostrar su nombre, anunciar artículos en función de sus intereses o de compras anteriores, etc., lo cual tiene mucho que ver con la información en ambos sentidos que veíamos antes, esto era imposible antes del comercio electrónico. Comparemos la posibilidad de cambiar los contenidos de un canal de televisión con los periódicos digitales".[20]

La naturaleza del comercio electrónico puede influir en la manera en que los gobiernos intentan alcanzar sus objetivos reglamentarios, si no los propios objetivos; porque pueden adoptar objetivos comunes en materia de reglamentación, especialmente cuando la

[20] **Ibid.**

actividad de que se trate se considere universalmente condenable. Son ejemplos de actividades de este tipo la difusión de pornografía infantil o de instrucciones para la fabricación de bombas o el blanqueo de dinero.

Si los Estados pueden llegar al acuerdo de que se trata de actividades inadmisibles, es relativamente fácil ver como pueden adoptarse en cooperación las disposiciones oportunas para la observación de las normas. Generalmente no se plantearían dificultades jurisdiccionales.

"Sin embargo existe una categoría de intervenciones reglamentarias que se refieren a las actividades que determinados gobiernos desearían prohibir pero respecto de las cuales no existe un consejo sobre las normas. Serían ejemplos de actividades incluidas en esta categoría una cierta pornografía y diversos tipos de publicidad. En estos casos, el gobierno que desee evitar que algo ocurra tendrá que basarse exclusivamente en su propia autoridad jurisdiccional o intentar obtener la cooperación de otras jurisdicciones. No obstante dada la naturaleza multijurisdiccional de las transacciones, pueden surgir complicaciones en cuanto a la observancia y la vigilancia. Por ejemplo, la transacción, puede originarse en un país en el que se permiten esas actividades y acabar en un país en el que no se permitan. La tercera categoría comprende las actividades que quizá sea necesario reglamentar pero que los gobiernos no desean prohibir. Más bien se trata de establecer condiciones previas para la participación en el mercado, por ejemplo prescripciones en materia de licencias, que quedan sometidas a lo dispuesto en la normativa de cada país. El objetivo reglamentario de estas medidas sería, por lo general, garantizar que los proveedores de servicios estén suficientemente equipados para

suministrar los servicios que ofrecen y que la calidad de los servicios suministrados sea de nivel adecuado. Por ejemplo, los gobiernos pueden desear garantizar que los médicos extranjeros que suministran servicios médicos transfronterizos por internet posean los títulos de aptitud necesarios. En este tipo de situaciones, la cuestión es, con frecuencia proporcionar información suficiente para proteger a los consumidores, y, como se ha dicho, una solución posible sería la participación indirecta de los gobiernos y la intervención de los proveedores y/o los consumidores, porque la naturaleza de los servicios y su modo de entrega también puede plantear problemas de observancia y vigilancia en esta esfera".[21]

Dadas las ventajas del comercio electrónico, en algunos casos los gobiernos quizá decidan renunciar a una cierta medida de certidumbre reglamentaria a cambio de un comercio eficiente y sin obstáculos. Será más probable que se considere favorablemente la posibilidad de modificar las prescripciones propiamente dichas. Otra consistiría en delegar funciones reglamentarias en aquellos que pudieran desempeñarlas de la manera menos invasora posible, por ejemplo, en los consumidores o en los proveedores, reservando al gobierno una amplia función de supervisión.

Como se puede apreciar, el comercio electrónico plantea algunas cuestiones jurisdiccionales relacionadas con la reglamentación que influye en la naturaleza y el contenido de cooperación intergubernamental; sin embargo, los objetivos reglamentarios pueden cumplirse en la fuente del suministro, en la jurisdicción de que proceden los productos de que se trata, en la jurisdicción en que tiene lugar el consumo.

[21] **Ibid.** Pág. 31.

"Estos enfoques compuestos plantean la cuestión fundamental de hasta qué punto están dispuestos los gobiernos a permitir que otros reglamenten las transacciones electrónicas transfronterizas que afectan a sus consumidores. Es probable que haya actitudes muy distintas, tanto según el gobierno de que se trate como según la naturaleza de la actividad. Cuando se adopte el enfoque basado en el modo 2 es decir, cuando la jurisdicción de los proveedores asuma la responsabilidad reglamentaria de todas las transacciones ello puede resultar ventajoso para los proveedores y los consumidores desde el punto de vista de los costos y de la sencillez de la observancia de las reglamentaciones. Pero en este enfoque está implícito el reconocimiento recíproco respecto de las tres categorías de reglamentación del contenido. Esto significa que, en lo que se refiere a estos tipos de transacciones transfronterizas, y suponiendo que no exista una armonización de las reglamentaciones, se permitirá a los consumidores elegir la jurisdicción en que desean realizar sus operaciones, en parte en función de la situación reglamentaria".[22]

Es de considerar que, incluso si este enfoque es aceptable y podría aducirse que, es la práctica, esa es la situación, por defecto, cuando los gobiernos no han intentado reglamentar o vigilar directamente el comercio electrónico procedente del extranjero; en sus propias jurisdicciones la cooperación internacional debe seguir desempeñando una función en relación con el suministro de información.

2.2. Antecedentes

El surgimiento de internet marca una nueva era de entendimiento entre los consumidores y

[22] **Ibid.** Pág. 33.

los proveedores y genera una expansión radical de los medios y alcances del comercio. La digitalización de las negociaciones es una respuesta muy natural si se atiende a que donde están las masas, está el comercio.

Antiguamente los mercados, lugares en donde se transaban las especies, se ubicaban en los centros de las ciudades, donde todos pudieran atenderle. A medida que el uso de internet crece, se vuelve evidente que el foco de intervención se modifica. Internet es el mercado del futuro y como tal da surgimiento al comercio electrónico como extensión inmaterial de estos antiguos antros. Sin embargo, la dinámica del antiguo comercio con el electrónico es la misma. Las repercusiones, empero, son las que se han modificado y con repercusiones se alude directamente a los beneficiarios. Ahora se puede decir con total propiedad que el intercambio de productos se realiza de muchos a muchos, a diferencia de un pasado en que el proceso se daba de uno a uno.

El comercio electrónico nace como expresión de la eficiencia y el ser más productivo. Como afán de satisfacer de forma integral nuevas necesidades, bajo el visor de la tecnología, que juega un papel esencial en su materialización. Es gracias a la revolución y vertiginoso auge de la tecnología de la última década que se ha hecho posible el anclaje del comercio electrónico. Y precisamente, es la tecnología la herramienta que cimienta el desafío más importante del rubro; el conseguir escoger las formas en que se requiere utilizarla, a fin de multiplicar los beneficios recogidos de los procesos productivos.

El desarrollo del comercio electrónico genera también riesgos derivados de los problemas inherentes a los sistemas digitales que sirven de instrumento para el intercambio de datos;

los cuales son susceptibles de usos, abusos y errores por personas no autorizadas que pueden provocar graves perjuicios. Estos riesgos se acentúan especialmente cuando el comercio se desarrolla en redes abiertas como internet.

"Solano Bárcenas afirma que la responsabilidad contractual en el comercio electrónico implica la presencia de numerosos protagonistas: servidores, usuarios, productores, transportadores, etc., cuyas relaciones contractuales no están enmarcadas por disposiciones legislativas específicas y que tienden generalmente a abusar de las cláusulas de no responsabilidad. Cavanillas Múgica por su parte, señala dos peculiaridades en el marco de la responsabilidad originada con motivo del tráfico informático: en primer lugar, la multiplicación de los eventuales legitimados pasivos, como consecuencia de la aplicación de la tecnología informática, siendo susceptibles de acción de responsabilidad, fabricantes, vendedores, empresas de mantenimiento de cada uno de los componentes del hardware de cada usuario, el suministrador del software, el intermediario electrónico, el propietario de la línea empleada, el concesionario de la misma, etc. En segundo lugar alude a la complejidad tecnológica de los medios empleados que puede en muchos casos impedir o hacer demasiado costosa la prueba acerca de la fase del circuito en la que se ha producido la disfunción. Por lo que, a la pluralidad de sujetos a responder, se agrega la dificultad en la identificación del causante".[23]

Con relación a los efectos de la contratación electrónica, hay que destacar que en la actividad telemática se plantea en la práctica, un gran problema para poder determinar tanto el daño como el hecho dañoso, dada la multiplicidad de elementos técnicos y

[23] Apoyo Consultores. **El comercio electrónico en Perú.** Pág. 99.

humanos que intervienen en cualquier rutina, por simple que sea; en este sentido, porque la víctima del daño causado puede ser tanto el propio titular de la red, como los sujetos que actúan en cada extremo de la línea; por lo que las principales dificultades en este ámbito, giran en torno a la relación de causalidad.

"El régimen de la responsabilidad aplicable en cada caso es como sigue:

a) A los proveedores de acceso o servidores: Dentro de los distintos intermediarios en la red, nos encontramos con el proveedor de acceso, con quien se contrata la conexión a la red y el centro servidor de información en la red, que comercializa información para poner en contacto a los intervinientes en el sistema de pagos, en este sentido, son agentes especializados en la prestación de un servicio.

b) Los intermediarios proporcionan servicios adicionales, haciendo operar la infraestructura de las telecomunicaciones sobre las que se realizan las transacciones, manteniendo sus respectivos convenios privados con el emisor, con el titular y el proveedor de bienes y servicios adherido al sistema de tarjetas.

c) El particular en nuestro caso titular de la tarjeta, generalmente contrata con un proveedor de acceso (aun cuando también lo puede hacer directamente con el servidor) la conexión a internet, quien le asignará sus correspondientes claves de identificación (login y password). El acceso al servicio se realizará mediante el código del cliente y el password que son claves personales e intransferibles generadas por la empresa proveedora que da acceso a internet, entendiendo que el cliente asume los riesgos por el quebrantamiento de la confidenciabilidad

y el mal uso de las claves y códigos de acceso. La pérdida de la información por culpa o negligencia del proveedor de acceso o del servidor, según los casos, será su responsabilidad, en tal sentido, la empresa deberá responder no sólo ante el cliente, sino también ante terceros de los daños y perjuicios que se deriven de la manipulación incorrecta o no autorizada, que puedan provocar averías o deterioros en el servicio o pérdida o destrucción de la información".[24]

Como se puede apreciar, en una operación de comercio electrónico, la relación que une al servidor con cada una de las partes se encuadra bajo la figura atípica de los denominados contratos informáticos; por lo tanto, se hace referencia a una responsabilidad contractual relacionada con todos aquellos elementos que forman el sistema, así como los bienes inmateriales que proporcionan las órdenes, datos, procedimientos e instrucciones, en el tratamiento automático de la información, la compraventa, el suministro, el mantenimiento y el arrendamiento de servicios digitales.

"De acuerdo al contenido del contrato y a la naturaleza de los servicios prestados, podríamos decir que la relación contractual que une al servidor con cada una de las partes involucradas, es un contrato de arrendamiento o prestación de servicios informáticos, donde el servidor se obliga a ejecutar una determinada actividad. En los términos indicados, el servidor (arrendador) de cada una de las partes, en este caso, del titular, del proveedor de bienes y servicios, y del emisor (arrendatarios), se obliga a prestar un servicio (interconectar y suministrar la información en la red) a los diferentes usuarios a cambio de un precio cierto, configurándose una relación de tracto sucesivo que puede ser

[24] Hernando, Isabel. **Seguridad y fiabilidad en el comercio electrónico: autoridades de certificación.** Pág. 33.

rescindida en cualquier momento por cualquiera de las partes".[25]

Es de señalar que de acuerdo a lo expuesto por los autores, la especialidad de los contratos informáticos radica en las obligaciones que asumen las partes; en este caso, además de las obligaciones propias del contrato de arrendamiento, el servidor o el proveedor de acceso, deben cumplir las obligaciones de información sobre el funcionamiento del sistema; para que el usuario pueda acceder a la información y manejarla correctamente, y prevención sobre los riesgos y asesoramiento técnico; estando obligado el usuario por su parte a colaborar con el desarrollo del contrato y cumpliendo con las instrucciones suministradas e informando al proveedor a tiempo sobre cualquier situación anómala.

Asimismo, se encuentra que el proveedor de los servicios de internet interviene en las operaciones del denominado comercio electrónico seguro; como tercera parte de confianza que emite certificados que, a la vez que sirven para distribuir la clave pública, sirve, de forma fundamental, para asociar de forma segura la identidad de una persona concreta a una clave pública determinada, por lo que el mismo se involucra, primero, con los emisores, segundo, con el suscriptor y finalmente, con el usuario.

De manera que tanto los titulares como los aceptantes de las tarjetas pueden contratar con los emisores en su función de proveedores de servicios de certificación; independientemente de su desempeño como emisores o propietarios de la marca de tarjeta o de cualquier medio de pago electrónico aceptada por los proveedores y disponible

[25] **Ibid.** Pág. 34.

en la red de internet.

Al haber explicado las características y particularidades del comercio electrónico y su importancia, se considera que el lector visualiza la tendencia que esta actividad tendrá en los próximos años y la importancia del mismo para la economía del país, con lo cual se encuentra que Guatemala, todavía tiene mucho camino que recorrer para contar con una plataforma digital que la ponga al mismo nivel de los países desarrollados, porque de lo contrario, la actividad productiva del país, especialmente la orientada hacia la exportación se contraerá, porque no tendrá las condiciones materiales ni tecnológicas para competir con los oferentes de otros países que tienen un mayor avance en el uso de la tecnología en sus actividades comerciales.

CAPÍTULO III

3. Los medios digitales para transacciones electrónicas

En la actualidad existe la necesidad de realizar transacciones financieras sin el intercambio de monedas o papeles, sino a través de redes electrónicas, manteniendo la premisa de conservar anónima la identidad de quien paga, ofreciéndole mayor comodidad y seguridad física.

Asimismo, para la utilización del comercio electrónico es indispensable salvaguardar la seguridad de las transacciones que se realizan, así como proteger en todo momento la privacidad de los usuarios de la internet. Sin embargo, existe un tema de igual o mayor importancia que los antes mencionados; que es el referido a la forma en que el dinero se traslada del comprador al vendedor; es decir, los medios de pago utilizados para que las transacciones electrónicas sean eficaces.

"Una transacción electrónica no es más que un contrato celebrado mediante medios electrónicos, a través de la red. La mayoría de las transacciones que se hacen por la red, son de compraventa donde el vendedor se obliga a transferir la propiedad de un bien al comprador, y éste a pagar un precio. El pago desde el punto de vista del comercio electrónico, es el mecanismo mediante el cual se ejecuta la contraprestación de una obligación asumida a través de la internet, es decir mediante la contraprestación electrónica."[26]

[26] Esteban, Francisco Javier. **La sociedad de la información electrónica.** Pág. 9.

En internet los medios tradicionales de pago no son efectivos, pues no es posible asegurar el envío de dinero de manera inmediata y confiable; por lo que para solucionar ese problema, existen los llamados medios de pago electrónico, aceptados, en la mayoría, por no decir en la totalidad de tiendas virtuales y páginas de la internet; los cuales agilizan las transacciones y procuran brindar la seguridad necesaria para llevar adelante el comercio electrónico.

3.1. Definición de los medios electrónicos de pago

Se puede entender como pago electrónico, aquel mecanismo mediante el cual se ejecuta la contraprestación de una obligación asumida a través de la internet; es decir, mediante la contratación electrónica.

"Según la segunda disposición de la Comisión de las Comunidades Europeas, el pago electrónico es definido como cualquier operación de pago realizada con una tarjeta de pista magnética o con un microprocesador incorporado, en un grupo terminal de pago electrónico o terminal de punto de venta".[27]

El pago como contraprestación por la obligación asumida en el comercio electrónico se caracteriza por ser únicamente en dinero, no pudiendo ser en especie, prohibición que se ha gestado por motivo de la costumbre comercial que impera en internet.

Se puede señalar entonces, que los medios de pago electrónico son mecanismos para

[27] **Ibid.** Pág. 29.

efectuar la contraprestación llamada pago, a través de la internet, ya que no es posible que el dinero en efectivo circule, por lo que se utilizan sistemas seguros que permitan al obligado a la contraprestación cumplirla cabalmente y al vendedor recibir el dinero por la prestación realizada, sea cual fuere la misma.

En función del momento de pago, cabe destacar que los medios son: de prepago, pago inmediato y pago diferido. Los primeros son aquellos en los que existe una conversión previa de dinero real a dinero electrónico antes de realizar transacciones, como por ejemplo los monederos electrónicos. Los de contraprestación inmediata, suceden cuando la transacción se efectúa en tiempo real, es decir con dinero en efectivo; mientras que en los de carácter diferido, el pago se realiza después de un determinado tiempo, como es el caso del pago con tarjeta de crédito; de igual manera, en función del soporte que utilizan se distingue entre el dinero almacenado en una tarjeta plástica y el generado a través de un formato de software.

"Después de revisar las diferentes propuestas en torno a la definición de un estándar de dinero digital, se considera que las siguientes características deben de incorporarse en cualquier propuesta de medio electrónico de pago:

- Universalidad: Todo dinero será válido y aceptado en todas partes de común acuerdo para pagar cualquier adquisición.
- Facilidad de uso: Que no resulte tedioso su uso, sino que sea tan práctico y rápido como sacar monedas del bolsillo.

- Seguridad: Se debe evitar que cualquier usuario pueda copiar, duplicar, reutilizar y falsificar el dinero, ya que todo lo digital es más propenso a éste tipo de detalles.
- Anonimato: Constituye sin duda uno de los aspectos más debatibles de los sistemas, ya que mientras algunas personas creen que es su derecho a la privacidad, para otras podría constituir una puerta abierta a la delincuencia y el lavado de dinero. La tendencia es proteger la privacidad del comprador, evitando que se pueda saber quién ha usado el dinero y para qué. Este aspecto ha sido descuidado en las tarjetas convencionales.
- Divisibilidad: La unidad de moneda digital debería ser fácilmente fraccionable para hacer pagos exactos, grandes o pequeños según se desee, es decir, que se tendrán disponibles varias denominaciones.
- Garantía: de la autenticidad del vendedor y que el pago no lo recibirá un tercero.
- Acreditación del pago: El otorgar un recibo de una transacción sería fundamental para evitar que alguna de las partes se desdiga de alguna acción, así mismo se respalde el pago por adquisición de un bien y/o servicio".[28]

En el futuro la utilización masiva de estos medios de pago, tendrán una importante repercusión en la política monetaria a nivel mundial y obligará a asegurar la estabilidad de los precios y la función del dinero. Sin embargo, para que estos medios sean totalmente eficaces, se necesita desarrollar normas que garanticen su funcionamiento, la confidenciabilidad de las transacciones y la adecuada protección al comerciante y sobre todo al consumidor final.

[28] Bueno Campos, Enrique Rafael. **La banca del futuro. Un desafío para el 2050.** Pág. 23.

3.2. Clases de medios de pago electrónico

Cuando se accede a una tienda virtual y se desea comprar algún producto, se puede observar que las operaciones de pago incluyen los siguientes medios: tarjeta de crédito, débito o cuenta corriente, etc., lo cual muestra que los billetes o las monedas tradicionales no tienen validez en la red informática. Siendo la tarjeta de crédito la forma más usada para realizar las transacciones telemáticas; lo cual se debe básicamente a su fácil uso, característica esencial de este medio de pago y por la seguridad que brinda tanto al vendedor, ya que existe una entidad financiera que respalda al consumidor, así como para el consumidor ya que frecuentemente las mismas se encuentran amparadas por seguros; asimismo, existe la confianza generalizada que las operaciones que se realizan utilizándolas, están más que probadas y cuentan con todas las garantías.

De igual manera, tienen mucha aceptación las tarjetas de débito, las cuales son plásticas, magnetizadas y numeradas, que sirven para realizar compras de bienes y/o servicios en las tiendas virtuales en las que se permite el uso de las mismas. "Estas tarjetas se encuentran asociadas a una cuenta de ahorros, y requieren para su uso que la cuenta disponga de fondos suficientes para comprar el producto y los gastos que ésta compra pudiera generar (envío por ejemplo). La verificación de fondos se produce antes de realizar la operación de compra por internet. Para realizar la compra, se debe digitar el número de la tarjeta y la fecha de vencimiento de la misma, previa verificación que la tienda acepte este tipo de tarjetas y que sea una zona segura".[29]

[29] **Ibid.**

También existe el dinero electrónico o digital, el cual es un sistema para adquirir créditos de dinero en cantidades relativamente reducidas. Este dinero electrónico se almacena en la computadora y se transmite a través de redes electrónicas para ser gastado al hacer compras electrónicas a través de internet; el cual, teóricamente, puede utilizarse para cancelar compras por montos pequeños, hasta décimas de centavo de quetzal o menos. Sin embargo, la mayoría de los comerciantes que aceptan dinero electrónico hasta el momento, lo emplean como una alternativa a otras formas de pago de adquisiciones de precio un tanto superior.

El dinero electrónico está pensado en la mayoría de veces para realizar pagos de objetos de precio no inferior a cincuenta quetzales; alternativa que es eficiente, ya que no se incurre en los costos que representan utilizar las tarjetas de crédito, sobre todo si se usan en volúmenes pequeños de dinero.

"El dinero electrónico funciona de la siguiente manera (para el consumidor): El primer paso es afiliarnos a un banco que ofrezca este sistema de dinero electrónico, luego debemos suscribir un contrato con alguna empresa proveedora del sistema, la cual nos proporcionará el software para instalarlo en la computadora. Este software permite bajar el dinero electrónico al disco duro de la computadora. La adquisición inicial se realiza contra nuestra cuenta bancaria o una tarjeta de crédito. Una vez instalado el software en la computadora, procederemos a realizar nuestras compras en la red, asegurándonos que la tienda virtual que escojamos acepte dinero electrónico o digital. Una vez escogido el producto y listos a realizar la compra, debemos simplemente hacer click en el botón de pago y el software resta la cantidad del precio y crea un pago que es enviado al banco,

verificado y luego depositado en la cuenta de la tienda virtual. Una vez que se ha concluido este proceso se notifica a la tienda virtual y ésta envía la mercancía que hemos comprado. Entre los sistemas de dinero electrónico o digital más usados en la actualidad tenemos el Cybercash, pariente de CyberCoin, E-cash y el sistema DigiCash".[30]

Hasta el presente, el dinero electrónico no se ha difundido debido a los problemas que supone su uso; como la instalación de programas en la computadora del comprador y la necesidad de una infraestructura especial en la tienda virtual del vendedor. Por este motivo, existen pocas tiendas virtuales que poseen estos programas por lo cual no se puede utilizar toda la red.

Asimismo, el mercado virtual ofrece las denominadas tarjetas inteligentes o smartcards, las que se caracterizan por tener una tecnología de pago considerada muy segura y respaldada por muchas instituciones financieras y empresas de tecnología. Entre sus características destacan su óptimo funcionamiento, ya que son eficientes, seguras, rápidas, así como aceptadas tanto en tiendas reales como virtuales, en muchas partes del mundo.

Otra opción que se ha incluido para las compras en internet es la tarjeta pre-pago, la cual sirve como medio de pago por las características físicas que posee; ya que puede ser recargable o de lo contrario se puede desechar si ya no existe un interés en su uso.

[30] **Ibid.** pág. 25.

"Esta tarjeta monedero es una tarjeta plástica que contiene un chip que almacena cierta cantidad de información en su memoria equivalente al monto de dinero que servirá para la operación, es decir al valor pre-pagado que posee la tarjeta, el cual se va descontando después de realizar las compras. Su funcionamiento es similar a las tarjetas pre-pago que conocemos, que se utilizan para activar los celulares. Es muy sencillo, cada tarjeta tiene un valor preestablecido, y posee una clave que identifica cada tarjeta. Cuando vamos a comprar en la internet, debemos fijamos que la tienda a la que recurrimos acepte estas tarjetas, de ser así, a la hora de efectuar el pago, ingresamos el número secreto de la tarjeta, y el precio se cancela respecto a nosotros, automáticamente. Luego la compañía que emite estas tarjetas paga el valor de lo acordado a la tienda virtual, utilizando políticas propias de estas compañías. En México, Visa Cash es la primera tarjeta monedero que se carga a partir de efectivo, o mediante una tarjeta de crédito o débito de banda magnética en terminales situados en sucursales bancarias, cajeros automáticos o terminales de carga atendidos".[31]

Como se puede apreciar, existen múltiples alternativas de pago en internet, con la finalidad que el usuario o consumidor adquiera bienes o servicios, en los establecimientos afiliados.

3.3. Desarrollo del comercio electrónico

Las pautas de compra de los productos y servicios de alto valor han cambiado radicalmente con la generalización y abaratamiento del uso de las tecnologías de información. En muchos productos físicos o presencial, el comprador debe cancelar el

[31] **Ibid.** Pág. 28.

costo del bien que adquiere a través de las formas de pago aceptadas legalmente, , siendo en el caso de las actividades mercantiles digitales, una forma innovadora de transar bienes y servicios, pudiéndose llevar a cabo la contraprestación del valor a través de un medio digital de crédito o débito. En la definición de esa oferta confluyen las empresas de distribución más eficientes y las entidades financieras, que se ven obligadas a diversificar sus líneas tradicionales de negocio por la creciente desintermediación.

"Los sectores de la distribución y el bancario, son los más afectados ente esta situación, por lo que los intereses de las entidades financieras y las empresas de distribución tienden a confluir más que en productos tangibles con servicios financieros y no financieros. La competencia es en la información, y esto abre un amplio campo de colaboración entre los sectores bancarios y de distribución que permitirá incrementar las sinergias del amplio y específico conocimiento que se tiene en cada uno de ellos sobre sus respectivas clientelas. Pero el manejo de la información implica nuevos riesgos, sobre todo en lo relativo al buen fin de las operaciones comerciales y los mecanismos de pago asociados a las mismas. La caracterización de esos riesgos y su minimización mediante acciones conjuntas de empresas de distribución y entidades financieras constituyen el objetivo de esta comunicación. La colaboración en este ámbito se muestra imprescindible, tanto para potenciar el desarrollo del comercio electrónico como para asentar la posición de mercado de unas y otras empresas ante la perspectiva integradora monetaria".[32]

[32] Sainz de Vicuña, José María. **La distribución comercial: Opciones estratégicas.** Pág. 28.

Dos factores que en mayor medida han impulsado el desarrollo del comercio electrónico son: los cambios de comportamientos de los consumidores o clientes y el desarrollo tecnológico.

Durante los últimos años se han producido una serie de cambios significativos en los hábitos de compra de los consumidores; motivados principalmente por cambios demográficos, culturales y de estilos de vida. Más concretamente, se ha incrementado el número de hogares compuestos por individuos aislados o parejas sin hijos, en las que trabajan los dos miembros y se ha acrecentado el envejecimiento de la población. Por otro lado, con la incorporación de las mujeres a la actividad productiva, se ha reducido el tiempo que las mismas tenían para ir personalmente al mercado o supermercado, siendo sustituida esta actividad por pedidos a través de Internet, lo cual permite un mayor volumen de los actos de compra, porque en poco tiempo puede adquirir mayor cantidad de productos de distintas tiendas virtuales, facilitándole surtir su despensa y maximizar el tiempo disponible para emplearlo en otras actividades que necesita hacer. Todo lo cual avala las enormes posibilidades de desarrollo del comercio electrónico, que permite mantener horarios ininterrumpidos de atención al público, para atender adecuadamente a estos nuevos comportamientos de los consumidores. Estos desean realizar las compras de bienes y servicios, financieros y no financieros, empleando el menor tiempo posible, a cualquier hora del día, e incluso de la noche.

Otro factor que ha contribuido a la modernización de la distribución comercial y la actividad bancaria ha sido el cambio tecnológico producido con la aplicación de nuevas tecnologías en ambos sectores. Así, la tecnología de la información, las aplicaciones de la informática

y la telemática y el uso de la transferencia electrónica de fondos ha supuesto una auténtica innovación en el comercio y la banca.

En definitiva, entre las posibilidades de la aceptación y difusión del comercio electrónico se encuentra el ahorro de tiempo que se produce en el acto de compra o de operación bancaria por evitar el desplazamiento y los amplios horarios de atención al público que mantiene; la posibilidad de disponer y analizar más información sobre la calidad y los precios de los diversos productos y servicios, por parte de los consumidores, cada vez más exigentes ante el aumento y diversificación de la oferta; y el desarrollo y la aplicación de las recientes innovaciones tecnológicas a la distribución de bienes y servicios, así como su difusión y aceptación entre los consumidores, que psicológicamente están preparados para estos nuevos canales de distribución.

"Esta nueva forma de distribución, mediante ordenador en red puede suponer una reducción del precio de los productos (hasta de un 60% en pocos años, según un estudio elaborado por Coopers & Lybrand), ya que se reducen los gastos de marketing, de almacenamiento, de intermediación (al eliminarse las funciones de determinados canales de distribución intermediarios, como el de los mayoristas) y sobre todo los costes de transacción y coordinación. Probablemente el comercio electrónico va a tener un fuere impacto en la cadena de valor tradicional, al desarrollar un nuevo modelo de relación entre el productor y el consumidor final".[33]

El comercio electrónico tiene la capacidad de matizar el valor de la proximidad que se

[33] **Ibid.**

atribuía a determinados pequeños comercios tradicionales, que en el sector financiero afecta igualmente a determinadas entidades, sobre todo las que basan su estrategia de negocio en una densa red de oficinas y la proximidad de las sucursales al domicilio del cliente.

En Guatemala, aunque no existen cifras oficiales, se ha visto un crecimiento de la cantidad de empresas, especialmente supermercados, que están utilizando las ventajas del comercio electrónico para presentar sus ofertas a los consumidores, que estos realicen su pedido y se lo llevan a su casa, utilizando como medio de pago electrónico únicamente la tarjeta de crédito y la de débito.

Las innovaciones tecnológicas al servicio del sector de la distribución, no sólo se manifiestan dentro del ámbito de la información y la comunicación; ya que además sirven de soporte de las transferencias electrónicas de fondos, lo que contribuye a la agilización, la comodidad y la interactividad en el acto de la compra; siendo precisamente ésta la forma de pago más utilizada en el comercio electrónico.

Partiendo de la premisa de que los cambios de comportamiento de los consumidores y las innovaciones tecnológicas constituyen factores fundamentales en el desarrollo del comercio electrónico, los recientes avances en materia de seguridad, en concreto, la creación de autoridades de certificación y protocolos de seguridad, así como la coordinación y colaboración entre los distintos agentes involucrados en este tipo de comercio, están favoreciendo su evolución.

El comercio electrónico ha supuesto así un cambio en la concepción convencional de la distribución total, caracterizado por la interactuación e integración de las funciones de distribución; como por ejemplo, la fusión de mayorista y detallista, las entidades financieras y los consumidores.

Todos los agentes implicados en el proceso requieren involucrarse en un entramado de relaciones comerciales y financieras, que pueden sintetizarse al describir brevemente sus respectivos papeles en la realización de las transacciones:

- El consumidor titular, quien es el comprador en una operación de comercio electrónico, que dispone de una cuenta bancaria, a la que se asocia una tarjeta de crédito o débito, se identifica mediante el número de tarjeta.
- La entidad financiera, emisora o el banco que emite la tarjeta que permite al titular el cargo en su cuenta; autoriza las operaciones y forma parte del sistema de autorización y liquidación de una marca de tarjetas.
- La empresa de distribución comercial, empresa que vende sus productos a través del comercio electrónico, y está afiliada al programa de tarjetas de crédito de una entidad financiera, quien dispone de un mecanismo para presentar al cobro las operaciones de tarjetas y se identifica mediante un número de afiliación o de cuenta.
- La entidad financiera adquiriente en la que la empresa de distribución comercial presenta las operaciones al cobro, porque es en la que ésta tiene la cuenta bancaria, la cual proporciona a la empresa de distribución el sistema manual o

electrónico que lo pone en contacto con el sistema de autorización y liquidación de una marca de tarjetas.

Para las entidades financieras, emisoras o adquirientes, su colaboración con las empresas de distribución abre nuevas oportunidades del negocio, que trascienden del mero papel de financiadores de operaciones del comercio tradicional. Desempeñar tales papeles les permitirá introducirse en el mercado del comercio electrónico, con unas inversiones relativamente bajas, que pueden garantizarles altas rentabilidades en el mediano plazo. No sólo podrán aumentar su cartera de clientes específicamente bancarios a través de la *banca electrónica que es un mercado en expansión*, sino que podrán captar nuevos clientes que deriven del propio crecimiento del mercado de la distribución comercial, que se introduzcan en el comercio electrónico y necesiten ser clientes de una entidad financiera que haga de adquiriente, como los consumidores de estos comercios, que para realizar sus compras electrónicas necesiten disponer de tarjetas inteligentes emitidas por una entidad financiera emisora.

Los consumidores de las empresas de distribución comercial pueden convertirse de esta forma en clientes de las entidades financieras que les posibilitan sus compras electrónicas, y que adicionalmente pueden proporcionarles créditos al consumo o cualquier otro servicio financiero adicional a la compra de los bienes y servicios. El comercio electrónico permitirá a las entidades financieras desempeñar sus funciones tradicionales mediante sistemas de menor coste que las redes de sucursales, pero también acceder a nuevos segmentos de clientes, con preferencias reveladas por nuevos canales de distribución y nuevas necesidades de productos y servicios financieros. Su colaboración con las empresas de

distribución no sólo es en beneficio de éstas, sino en el de los consumidores y en el de sus propias actividades financieras.

La aceptación y difusión del comercio electrónico en la actualidad se debe principalmente a los cambios en los comportamientos de los consumidores clientes, cada vez más exigentes, que valoran en mayor medida el ahorro de tiempo y la posibilidad de disponer y analizar más información sobre la calidad y los precios de los diversos productos y servicios. La generalización del comercio electrónico se ve impulsada por el desarrollo de las innovaciones tecnológicas y su difusión y aceptación entre los consumidores; así como por los recientes avances en materia de: seguridad en las transacciones y por la coordinación y colaboración entre los distintos agentes involucrados es ese tipo de comercio.

Con el comercio electrónico, que se hace operativo mediante los ordenadores conectados a redes telemáticas los servicios financieros pasan a integrarse con el estilo de vida del cliente, que puede realizar sus compras y transacciones bancarias, pagar sus recibos, encargar cheques de viaje, comprar y vender valores, entre otras muchas operaciones, a cualquier hora del día o de la noche.

El comercio electrónico permite así un sistema de oferta global o distribución total, caracterizada por la interactuación de las empresas de distribución, las entidades financieras y los consumidores.

Como se ha leído, en este capítulo se llevó a cabo la explicación de los elementos que particularizan y definen a los medios digitales utilizados en las transacciones electrónicas, la manera en que las tarjetas de débito y crédito se han convertido en una nueva manera de entender el dinero, así como la paulatina sustitución de la moneda metálica y en papel por el efectivo digital, con lo cual se puede asegurar que los procedimientos electrónicos sustituirán al papel moneda en todas los intercambios mercantiles de importancia en el país en los próximos diez años.

CAPÍTULO IV

4. El fraude electrónico

Los avances en la informática y las telecomunicaciones han orientado asimismo las estrategias bancarias hacia un mayor y más rápido aprovechamiento de las innovaciones tecnológicas (como los dispositivos de autoservicio, el teléfono, el ordenador o internet) para diseñar nuevos productos o servicios; inviables sin la existencia de estas nuevas tecnologías.

Ello también ha permitido el seguimiento de estrategias de segmentación de clientes, fundamentales en la sociedad orientada al cliente. En una primera etapa de utilización de las tecnologías de la información, algunas entidades de crédito, para adaptarse a los nuevos comportamientos de sus clientes, han ampliado sus canales de distribución de productos y servicios financieros.

En este sentido, las nuevas tecnologías les ha permitido utilizar al comercio como canal de distribución, instalando cajeros automáticos o empleando la banca telefónica para crear autoservicios financieros para los consumidores actuales; que tratan de optimizar la utilización del tiempo, ser cliente de una gran superficie y a la vez de una entidad financiera asociada a ésta; les puede proporcionar ventajas derivadas del ahorro de desplazamiento adicionales y de los amplios horarios de apertura de las empresas de distribución comercial.

Posteriormente, con el comercio electrónico a través de los ordenadores conectados a las redes telemáticas, como es internet, los servicios financieros pasan a integrarse con el estilo de vida del cliente, superándose la concepción tradicional del papel de la banca. Se trata de una forma alternativa de entender y realizar las actividades bancarias en un entorno económico en el que las fronteras intersectoriales tienden a desaparecer.

Los clientes desean seleccionar, encargar y pagar sus compras, realizar sus transacciones bancarias, pagar sus recibos, encargar cheques de viaje, comprar y vender valores, así como muchas operaciones, a la hora y en el lugar más conveniente según sus estilos de vida. Por tanto, la competencia de estas nuevas formas de distribución de productos financieros y no financieros converge en las tecnologías de la información.

El futuro inmediato del sector bancario se encuentra en la banca telefónica y electrónica, que permite ofrecer precios mucho más competitivos al lograr reducciones de costes superiores al 50% respecto de la operativa tradicional, ya que supone una importante reducción de los costes de transacción y coordinación. Ello mermará las oportunidades de beneficio de las empresas ineficientes, exigiéndoles un cambio en sus estrategias. La incorporación de las nuevas tecnologías a la actividad bancaria continuará definiendo un negocio financiero más complejo, mejorando la dimensión, las infraestructuras y las características propias de los bancos.

4.1. Desarrollo del fraude electrónico

Sin embargo, así como se ha generado el uso de la banca electrónica, los fraudes por

medios electrónicos han crecido exponencialmente en los últimos años. La inminente necesidad de usar internet como medio de comunicación prioritario ha abierto la puerta a múltiples estafadores que lo usan como un nuevo medio para atacar y defraudar a usuarios y empresas por igual.

El objetivo principal de un estafador normalmente es tener acceso a información de valor como cuentas bancarias, números de tarjeta de crédito, contraseñas y demás, con el objetivo de transferir dinero, hacer cargos o accesar a datos privados de los cuales puedan sacar algún beneficio.

"Pasemos a analizar las tendencias que han favorecido el desarrollo del fraude.

- Mayor presencia del crimen organizado. Se trata de pequeñas mafias, dos o tres individuos, cuya actividad empresarial es dedicarse a encontrar objetivos fáciles. En efecto, el crimen organizado podría ser responsable de la gran mayoría de los fraudes extremos, recordando siempre que estos sólo pueden ser exitosos con la participación interna de un empleado.
- La aparición del pirata informático, quien es aquella gente bien preparada, muy conocedora de los negocios y de los mercados, que considera que lo importante es ganar dinero a costa de lo que sea.
- Desarrollo de técnicas más asequibles de falsificación. La tecnología ha permitido lograr verdaderas maravillas que no tienen aquel aspecto artesanal de antaño.
- Más oportunidades de fraude por errores operativos. La necesidad de crecer y de ganar nuevos mercados, ha llevado a algunas empresas a reducir erróneamente

los gastos. Lanzan nuevos productos sin realmente tener buenos procedimientos operativos, ni contar con una buena formación para los empleados que van a vender, administrar y procesar esos productos.

- Fraudes multi-jurisdiccionales. Esa tendencia se viene observando sobre todo en los grandes fraudes. Esto ocurre cuando un fraude se realiza en un país A y los fondos son transferidos a una país B.
- Defraudadores dispuestos a presentar batalla legal. La inefectividad en la acción legal por parte nuestra hace que el defraudador se salga con la suya, incluso, a veces el defraudador se va contra la empresa, alegando daños y perjuicios.
- La forma más común de fraude electrónico se conoce como phishing. Esta técnica consiste en enviar mensajes de correo electrónico que simulan ser provenientes de bancos prestigiosos, subastas por internet o tiendas departamentales. Los correos incluyen enlaces a sitios fraudulentos que están diseñados tan similares a los sitios reales que es fácil confundirse. Estos sitios solicitan que ingrese o actualice información personal para después ser enviada a los estafadores a cargo del sitio".[34]

Una técnica común para introducir virus o programas informáticos que les permite a los estafadores obtener información de los usuarios; es por medio de descargar de forma automática aplicaciones cuando éste entra a un sitio web, a partir de que existen aplicaciones que se instalan automáticamente sin solicitar confirmación del usuario; utilizando fallos del navegador o aprovechándose de que no tiene criterios de seguridad adecuados.

---

[34] Novoa Monreal, Eduardo. **Derecho a la vida privada y libertad de información: un conflicto de derechos.** Pág. 106.

Una vez instalados estos invasores puede ser muy difícil quitarlos, terminando en ocasiones con la necesidad de reinstalar el equipo. Estos programas les permite a los defraudadores conseguir información personal y confidencial, incluyendo contraseñas de acceso a sistemas bancarios.

4.2. Actitud relativa frente al fraude

La actitud de las personas y empresas frente al fraude suele ser reactiva. Más de la mitad de los fraudes en las empresas son descubiertos por coincidencia; ya sea por información obtenida por medios externos, accidentes o cambios en la administración, entre otros factores.

"Por lo general, los directivos de las empresas tienen un conocimiento muy limitado de las operaciones en los negocios principales y, en menor grado, de sus operaciones en otros países. Así mismo, se observa cierta falta de coordinación en lo que se refiere al manejo de la información entre las subsidiarias y la casa matriz. Los directivos tienden a delegar la responsabilidad de implementar controles para prevenir grandes fraudes. La mayoría piensa que los auditores deben poder detectar los fraudes substanciales como parte de sus auditorías normales, a la vez que no están dispuestos a pagar más por pasarles la responsabilidad a sus auditores. Lo anterior sugiere que la gerencia debe asumir plenamente la responsabilidad o admitir que en el momento se le está delegando a la gente equivocada".[35]

[35] **Ibid.**

La gran mayoría de personas desconoce los procedimientos que realizan los estafadores para alcanzar sus objetivos; principalmente porque los bancos y las empresas de las que son usuarios no llevan a cabo campañas informativas sobre los mecanismos y procedimientos realizados por los estafadores para lograr sus objetivos; especialmente si consideran que pueden afectar su prestigio y la confianza del cliente hacia ellos.

4.3. Tipos de fraude

Las causas del fraude, en general, son internas y externas. Los fraudes internos son aquellos perpetrados contra una compañía o sus administradores u otros empleados. Los planes externos del fraude, por otra parte, se dirigen contra las compañías y son realizados por individuos o entidades, tan diversos como usuarios, beneficiarios, vendedores y criminales de carrera.

El fraude interno frecuentemente involucra el hurto de información privilegiada u otra propiedad de la compañía; relaciones inadecuadas con vendedores o asesores que llevan a conflictos de intereses; la desviación de fondos de los asegurados o de la compañía por los mismos empleados; el uso de información confidencial o la tergiversación intencional por agentes a posibles clientes sobre las características de los productos de la compañía.

El fraude externo involucra acciones que surgen fuera de la empresa pero que de igual manera persiguen obtener los recursos financieros o información valiosa de la misma.

4.4. Modalidades de fraude con tarjetas de crédito

La mayor cantidad de ilícitos son cometidos en relación con las tarjetas de crédito, porque las mismas implican el acceso a dinero virtual disponible todo el tiempo.

"En primer lugar, está el aumento de los cupos de tarjetas de crédito para luego hacer retiro mediante efectivo en cajeros o compras. Posteriormente vuelven a modificar los cupos como estaban anteriormente, como operaciones ficticias que afectan directamente a la empresa, pues aparentemente entra pero no existen en las arcas de la entidad. Esta modalidad se ha preferido en los últimos años, pues debe haber una persona dentro de la entidad para poder hacer la transacción con la cuenta ficticia, quien por esta operación recibe un importante porcentaje de comisión. También se crean programas ficticios dentro de un programa de información, desde donde se hacen desvíos de dinero, sacan de una cuenta bancaria y la desvían a alguna cuenta-objetivo determinada para tal ilícito. Aunque no se conoce con exactitud el número de casos de ilícitos realizados a través de los sistemas electrónicos, los organismos de investigación, han detectado diversos casos que involucran bandas organizadas alrededor del ilícito".[36]

El modus operandi de los delincuentes consiste en aumentar exageradamente el cupo de tarjeta de crédito, a través de modificación de registro de la misma en el sistema de cómputo, hasta terminar por completo la cantidad asignada ilícitamente, para luego entrar nuevamente al sistema en donde realizan los pagos de los créditos y bajar el cupo como se encontraba inicialmente; lo cual puede ser posible gracias a la colaboración de

[36] Arias de Rincón, Mauro. **La protección al consumidor en el comercio electrónico.** Pág. 41.

funcionarios o exfuncionarios, asociados con algunos tarjetahabientes, que prestan sus cuentas para ser clonadas luego de la transacción del dinero por parte de la entidad. A partir de esta experiencia las entidades financieras han comenzado a reportar sospechas por fraudes que involucran personal de la misma entidad.

"También se han creado mecanismos para robar la información contenida en la banda magnética, conocida como clonación de tarjetas, la cual inmediatamente que pasa por el datafono, desde el mismo sistema se sabe todo el contenido de la banda magnética, luego es quemada en otra banda, o hacen un montaje de prepago para servicio telefónico celular. Después en los lugares de fachada pasan la tarjeta por montos considerables que tengan un cupo elevado para así copiar la información. Hacen una plaqueta sobre la información de la tarjeta y después el voucher prepago lo pasan varias veces por ese lado, quedando como si la persona hubiera hecho la transacción".[37]

"La tarjeta caliente es aquélla que utilizan los delincuentes antes que el tarjetahabiente mismo llame a la entidad para pedir que la bloqueen por pérdida o robo. Este tipo de fraude es muy común, especialmente en supermercados y oficinas. También se encuentra la tarjeta alterada, la cual es un fraude que se comete con tarjetas plásticas cuya información se ha modificado total o parcialmente. Los delincuentes toman la tarjeta, construyen una cédula falsa y le cambian el número. Ellos conocen y calculan el dígito de chequeo y todo este tipo de cosas, consiguen números válidos de personas influyentes que tienen bastante cupo, cambian el nombre y empiezan a utilizarlas".[38]

[37] **Ibid.** Pág. 53.
[38] **Ibid.** pág. 55.

En el mercado guatemalteco se ha presentado el caso del uso de comprobantes previamente elaborados; lo cual sucede cuando se imprimen los comprobantes con elementos diferentes de la misma tarjeta, se distribuyen en comercios debidamente autorizados y pasan como auténticos; o bien, se hace uso de la falsificación de la banda magnética, por medio de lo cual se obtiene la información de una tarjeta, se graba y luego la puede leer un datafono; o bien, que en el negocio se produzca una doble facturación, cuando la persona paga la cuenta con tarjeta de crédito, pero el mesero pasa la tarjeta dos o tres veces, y luego trata de imitar la firma del cliente en los otros dos recibos.

Además, suceden prácticas negligentes de los mismos usuarios que imprudentemente escriben el código de acceso; por ejemplo, en la misma tarjeta plástica para no olvidar el número, facilitando el fraude ante una posible pérdida, atraco o paseo millonario.

Existe también la utilización de tarjetas legítimamente elaboradas por el banco, pero las entidades reciben documentación falsa, en donde el delincuente abre una cuenta con datos y nombres falsos y el banco, por fallas de análisis de crédito y de la documentación, le expide la tarjeta.

Ha sucedido que el estafador suplanta al tarjetahabiente en el proceso de recepción de la tarjeta; en donde, en unión con el empleado del banco, presenta una cédula falsa y reclama la tarjeta, pero el cliente real nunca la recibe.

"Otros tipos de fraudes son: la tarjeta gemela, ésta es exactamente igual a otra que ha sido emitida legítimamente por una entidad, teniendo en consecuencia, las mismas

características en materia de seguridad, calidad e información, incluidos los datos procesados en la banda magnética. Esta modalidad es difícil de detectar, excepto cuando se recupera el plástico utilizado para el fraude y puede corresponder a procesos de doble emisión en la misma entidad, por actividad dolosa de funcionarios que tienen que ver con esta etapa del proceso. Hay empleados que, en sus centros de realce, hacen una tarjeta para el banco y otra para ellos, por lo que los datos son auténticos y absolutamente iguales. Hasta el día de hoy la cédula de vecindad o el nuevo documento personal de identificación no es un problema pues hay delincuentes que por mínimo dinero solucionan tal inconveniente; esta modalidad es difícil de prevenir, sólo teniendo cámaras en los centros de realce o cuando se captura la tarjeta se puede detectar el fraude". [39]

Aún con estos fraudes, en internet se presentan grandes oportunidades económicas lo cual se incrementará en los próximos años. La penetración de esta herramienta está creciendo rápidamente en toda América Latina y para nadie es un secreto que muchos negocios del futuro se darán en línea; por lo que realizar transacciones vía internet es la obsesión de la mayoría de las empresas para volver más eficientes sus relaciones con proveedores, clientes corporativos y consumidores finales. La venta de libros, música, software, computadoras y muchos artículos más está cambiando por causa del fenómeno que se llama comercio electrónico.

Muchas empresas en Guatemala ya empezaron a moverse en el comercio electrónico, todo como respuesta a un profundo cambio en la cultura de los negocios. Internet dejó de ser un gran libro lleno de enlaces, imágenes e información estática para convertirse en un

[39] Martín Peña, Ricardo. **Exposición de una operación de comercio electrónico seguro con una tarjeta bancaria.** pág. 115.

medio de convergencia cultural, centro de ocio interactivo, comercio electrónico y transacciones comerciales.

Pero, aunque el comercio electrónico por internet es una gran alternativa, muchos usuarios se muestran reacios a realizar transacciones debido a los riesgos de seguridad en una red abierta y pública; en la cual los usuarios deben enviar sus números de tarjeta de crédito, datos financieros e información personal, una estadística poco alentadora para las empresas que están apostando al negocio de ventas en línea.

"En la actualidad, se han desarrollado mecanismos para ofrecer seguridad en internet, como los protocolos de seguridad SSL (Secure Sockets Layer) y SET (Secure Electronic Transations), certificados digitales y firmas digitales. Además, muchas compañías están aplicando políticas de seguridad y confidencial de información que permitan garantizar un alto grado de confianza a sus clientes, entonces, ¿Cuál es el problema de realizar transacciones y pagos en la red? En primer lugar, son pocos los países que han implementado la tecnología SET. Esto se debe a la dificultad de convencer y poner de acuerdo a todos los entes que participan en el proceso, comercio, bancos, entidades de certificación y terceras compañías que realizan procesos específicos (podrían ser los mismos bancos) que aseguran que los comerciantes y clientes son entes certificados y reconocidos. Así mismo, ante las barreras culturales de desconfianza, inseguridad e incluso ignorancia en el tema, la solución es conocer los procedimientos y recomendaciones para realizar una transacción segura en la red. Además, las compañías que ofrecen servicio de ecommerce y las entidades financieras deben consolidar

soluciones seguras de comercio electrónico y crear una cultura de confianza que permita una rápida expansión de estos servicios".[40]

Es de tomar en cuenta que hasta el más sofisticado esquema de seguridad es vulnerable, ya que todos ellos se diseñan para permitir el acceso a personas dentro de las compañías (ingenieros, programadores, administradores de red y demás). Esto debido a que las tecnologías actuales no pueden cubrir requerimientos muy importantes de seguridad; como el de la violación a los derechos de propiedad intelectual, extorsión, difamación escrita, infidelidad de empleados o fraude.

El progreso del comercio electrónico en Guatemala, como en otras partes del mundo, dependerá de inversiones en tecnología y alianzas entre los empresarios del comercio y las entidades financieras. Los acuerdos entre estos dos agentes para implementar sistemas de comercio seguros serán la clave en el futuro.

Las empresas deben recurrir a los grandes avances tecnológicos para incrementar la seguridad de sus actividades y garantizarles una adecuada protección a sus clientes virtuales; a partir de implementar procesos que consisten en máquinas computarizadas que puedan reconocer las características personales que un simple control no logrará. Ese reconocimiento puede estar en las huellas digitales, la disposición de los vasos sanguíneos en la retina del ojo, patrones de voz, y hasta el ritmo con que se escribe a máquina.

[40] **Ibid.** Pág. 117.

Estos mecanismos de seguridad en las nuevas computadoras, tienen sensores especiales que reciben las características, las convierten en un código digital y las comparan con los datos memorizados para lograr una total correspondencia entre los datos así contenidos y la persona a quien se presume le pertenecen esas determinadas características; su uso garantizará que mayor cantidad de personas acudan al comercio electrónico.

Al haber caracterizado el fraude electrónico, se puede comprender que el mismo es una modalidad de delincuencia, adaptada a las nuevas realidades que presenta el mundo en general y el país en particular; en donde los ilícitos se encuentran más avanzados que la legislación orientada a penalizarlos; así como las limitantes que enfrentan los Estados para combatir este flagelo, debido principalmente a la falta de expertos en las filas policiales y del Ministerio Público que puedan explicar la forma de operar de los hacker y demás piratas informáticos; especialmente quienes se orientan a una de las modalidades de fraude electrónico.

Aun cuando en Guatemala se han llevado a cabo denuncias de fraude electrónico, especialmente de la práctica del phishing; que es una técnica consistente en enviar mensajes de correo electrónico que simulan ser provenientes de bancos prestigiosos, subastas por internet o tiendas departamentales, incluyendo los correos enlaces a sitios que están diseñados a través de procedimientos fraudulentos; tan similares a los sitios reales que es fácil confundirse; así como la denominada clonación de tarjetas, que implica a una o más personas, quienes al recibir la tarjeta de débito o crédito del consumidor, la aplican más de una vez en el registro digital, para que el comprador pague el doble de lo

que realmente gastó, quedándose el que realiza este ilícito con el monto descargado, para comprar otros productos y que los pague el tarjetahabiente.

A pesar de esta tendencia, la legislación penal guatemalteca todavía no regula este tipo de ilícitos, ni como fraude electrónico propiamente, aun cuando se han regulados delitos vinculados con la informática, los cuales se encuentran desde el Artículo 274 "A" hasta el 274 "G" del Código Penal guatemalteco, Decreto número 17-73 del Congreso de la República.

Si se entiende al fraude como una acción que resulta contraria a la verdad y a la rectitud, cometida en perjuicio de otra persona individual o jurídica, se comprende que esté orientado a lo electrónico, implica que el hecho se orienta hacia prácticas contrarias a la verdad cibernética, como el caso de la clonación, en donde la verdad es que el consumidor únicamente realizó un gasto, el cual es el que debe descontársele, mientras que en el caso del phishing, sería la mejor ejemplificación de una conducta en contra de la rectitud, puesto que con prácticas ajenas a aquélla, se engaña a la persona aprovechándose de su buena fe.

CAPÍTULO V

5. Importancia jurídica de implementar medidas de seguridad en los medios digitales para transacciones electrónicas

Las medidas de seguridad tienen por objeto el estudio de la protección de los consumidores en las transacciones electrónicas de pago a la luz de las experiencias que se han tenido en relación a los fraudes electrónicos. Para determinar los derechos del consumidor en este aspecto se analizan los mecanismos de seguridad, tanto técnicos *como jurídicos que deben estar presentes en una transacción de pago. Un mecanismo de* pago seguro debe garantizar la confidencialidad y la privacidad de la operación, la indicación del riesgo y la determinación de responsabilidad por usos fraudulentos o no autorizados.

La seguridad en los sistemas de pago es considerada un elemento decisivo para el desarrollo del comercio electrónico; entre las cuestiones más importantes en este ámbito destacan la necesidad de garantizar la seguridad jurídica de la transacción, la privacidad de la operación y la prevención sobre el uso fraudulento de los medios de pago.

Por eso es que junto a sus innegables ventajas, el comercio electrónico, especialmente los mecanismos de pago digital, precisan la mayor coordinación posible entre los diversos agentes, sobre todo a nivel de flujos financieros y logísticos y para garantizar un nivel adecuado de seguridad y confidenciabilidad en las transacciones. De hecho, sin una íntima conexión entre grandes superficies y entidades financieras el problema de la seguridad

puede afectar estratégicamente el desarrollo efectivo de esta modalidad mercantil telemática.

"Dentro del contexto global del comercio electrónico y de las redes abiertas, las empresas de distribución comercial, las entidades financieras y los propios clientes, exigen cada vez unas mayores y más absolutas garantías respecto a cuatro aspectos fundamentales que se consideran irrenunciables:

a) La autenticación de los elementos integrantes en una transacción electrónica, con lo que se pretende asegurar que quien se comunica es quien dice ser.
b) La integridad de la transacción: para asegurar que el mensaje (o transacción) no ha sido modificado, alterado o manipulado.
c) La confidencialidad de la transacción: para que sólo tengan acceso a la lectura del mensaje aquellos que han sido previamente autorizados.
d) El no repudio de la transacción: con lo que se pretende asegurar que el mensaje, una vez aceptado, no pueda ser rechazado".[41]

Todas estas garantías de seguridad toman especial relevancia en las transacciones de índole económica y comercial. Precisamente, la expansión del comercio electrónico se ha visto frenada principalmente por el vacío legal existente en el comercio electrónico; no sólo por la carencia de una regulación apropiada para la operación financiera de pago en la transacción comercial electrónica, sino también por la falta de regulación del documento electrónico, de la designación del tribunal en caso de conflictos y de la inexistencia de

[41] Inza, Juan. **Comercio electrónico. Cómo deben preparase las entidades financieras.** Pág. 23.

registros e instituciones en las que comprobar la solvencia e identidad del negociante, entre otra lagunas legales; y que la seguridad requerida en materia de control de la confidencialidad e identificación del cliente, se está resolviendo mediante la utilización de códigos secretos de identificación personal.

En este sentido, la acreditación de la identidad e integridad de los documentos se puede realizar mediante la firma electrónica; ya que ésta se basa en algoritmos criptológicos de clave asimétrica, que es un sistema que protege con una clave secreta los datos. La encriptación también sirve para garantizar el secreto en las comunicaciones en internet.

"Cuando se realizan operaciones financieras, la seguridad se convierte en un elemento imprescindible. La inseguridad de los pagos y cobros a través de internet ha sido la principal traba para la masificación del comercio electrónico a través de la red, ya que se han planteado una serie de interrogantes: ¿Cómo cobrar ese producto o servicio? ¿Y en qué moneda? ¿Es internet seguro para las transacciones? ¿Cómo se puede estar seguro de la fiabilidad de los datos facilitados por el cliente? ¿Y de los del vendedor anónimo? ¿Cómo asegurarse de recibir la mercancía? ¿A quién reclamar en casos de incumplimiento?. Para resolver todas estas cuestiones relativas a la seguridad del comercio electrónico, han surgido las llamadas Autoridades de Certificación, cuyo objeto consiste en constituirse en esa necesaria tercera parte confiable, donde todos los elementos integrantes de comunicación segura a través de redes abiertas confían y se confían recíprocamente. Esta tercera entidad facilita mediante el uso de claves asimétricas, protocolos estandarizados de seguridad, criptografía y firma digital, los certificados electrónicos, esto es, la imprescindible confianza en esa tercera parte para

asegurar la identidad de los participantes y el más absoluto secreto de sus transacciones. De ahí su denominación más extendida: el notario electrónico."[42]

Para garantizar, igualmente, un nivel de seguridad adecuado en las transacciones monetarias, se han desarrollado protocolos de seguridad, los cuales permiten el pago seguro mediante tarjeta de crédito, porque garantiza la inviolabilidad de los datos transmitidos a través de internet, autentifica a las partes involucradas en una compra en línea y mantiene la privacidad de los detalles de los números y transacciones con tarjetas de crédito cuando se envían a través de una red; de tal manera que cada uno de los intervinientes sólo tiene acceso a los datos que necesita y no tiene acceso al resto. Su objetivo consiste, por tanto, en que nadie pueda interceptar una tarjeta y usarla fraudulentamente, y que nadie pueda alterar los mensajes que circulan por la red. Para lograr estos objetivos, utiliza encriptación de mensajes (sistema que protege con una clave los datos), firmas digitales y certificados criptográficos.

En el comercio electrónico el cliente emite, para el pago de un producto, una clave pública, previamente creada en función de una clave secreta o encriptadas que son secuencias de números y letras, que revelan la identidad de los clientes y sus números de cuenta, las cuales sólo pueden ser descodificadas en función de otras claves, también secretas, que poseen las entidades independientes que actúan como autoridades de certificación.

El concepto de seguridad en las transacciones electrónicas es amplio y abarca fundamentalmente aspectos técnicos y jurídicos; puesto que la seguridad jurídica implica la

[42] **Ibid.**

definición de los derechos y obligaciones de las partes a efecto de determinar a quién corresponde la responsabilidad en caso de una determinada actuación; también comprende la protección del derecho a la privacidad y la confidencialidad de la operación.

La seguridad técnica constituye una herramienta fundamental al auxilio de la seguridad jurídica; la tecnología ofrece diversos mecanismos que facilitan el cumplimiento de las obligaciones de seguridad impuestas a los proveedores, los métodos de cifrado son ejemplo de ello, ya que permiten ocultar la información, proporcionando la confidencialidad y privacidad de la operación; requisitos exigidos por la ley para garantizar la protección de los consumidores y usuarios.

5.1. La implementación de medidas de seguridad en los medios digitales para transacciones electrónicas para evitar que terceros lo utilicen para cometer fraude en perjuicio del tarjetahabiente

Uno de los aspectos más importantes relacionados con la protección de los consumidores se relaciona con la obligación de suministrar mecanismos de pago seguros. Para determinar el contenido de este deber, es necesario establecer los requisitos mínimos de seguridad que deben rodear las operaciones de pago para entender que éstas son seguras.

"En entornos electrónicos, la seguridad en los pagos debe ser estudiada desde un doble aspecto: el técnico y el jurídico. Desde el punto de vista técnico es importante el análisis de los métodos de cifrado de la información, los protocolos de seguridad y otras soluciones

que permiten efectuar pagos de forma segura. La seguridad jurídica precisa el estudio de la actuación de cada uno de los sujetos que intervienen en la transacción a efecto de determinar a quién corresponde la responsabilidad en caso de fallos técnicos, violaciones a la privacidad, operaciones no autorizadas o fraudulentas u otras transgresiones en el cumplimiento de los deberes impuestos por normas legales o contractuales".[43]

En la actualidad, existen diversos medios para proveer seguridad a las transacciones electrónicas realizadas a través de internet. Desde el punto de vista técnico, los mecanismos de seguridad se encuentran en la implantación de sistemas criptográficos que permiten el cifrado de la información, en el uso de firmas electrónicas y en los protocolos de seguridad, algunos de ellos diseñados específicamente para proteger los sistemas electrónicos de pago.

Por ello es que se considera válido exigir que los servicios de seguridad dentro del comercio electrónico proporcionen garantías fundamentales como la autenticación, la integridad, la confidencialidad y la aceptación de los mensajes de datos.

La autenticación se refiere al proceso de verificación de la identidad del remitente del mensaje de datos; esto es, que quien envía el mensaje sea realmente quien dice ser y no otra persona, con lo cual se evita supuestos de suplantación de identidad, permitiendo comprobar que los participantes en la operación comercial son quienes dicen ser. Gracias a este servicio, el comprador sabe de modo totalmente seguro en qué comercio está

[43] **Ibid.** Pág. 37.

comprando y el proveedor de bienes y/o servicios en internet puede estar seguro que quien está comprando es realmente el titular del instrumento de pago.

La integridad garantiza que los mensajes son recibidos sin alteraciones no autorizadas, es decir que no han sido modificados, alterados o manipulados durante la transmisión. En materia de pagos efectuados por medios electrónicos, este servicio avala la exactitud de los datos impidiendo que el comprador o el vendedor puedan alegar condiciones diferentes a las pactadas como sería, por ejemplo, una variación en el monto del precio.

La aceptación adquiere singular importancia, ya que impide que el comprador niegue el mensaje enviado autorizando el pago a través de su tarjeta u otro instrumento electrónico o que el vendedor niegue haber recibido el pago.

El mecanismo para garantizar la seguridad electrónica, consagra un conjunto significativo de dominios que pretenden establecer un ciclo de garantías lo más completo posible, advirtiendo que no todos ellos tiene impacto jurídico.

La comprensión de la finalidad y de los procesos involucrados en la aplicación de la norma internacional de seguridad; es un requisito fundamental para la adecuada contribución desde el derecho al sistema de gestión de seguridad de la información, tanto para los bancos, las empresas que ofertan en internet y al usuario; tema que no puede obviar el operador jurídico que como consultor intervenga, porque implica lidiar con la protección de datos personales; la contratación de bienes informáticos y telemáticos; el derecho laboral y prestación de servicios, respecto de la regulación de aspectos tecnológicos; los servicios

de comercio electrónico; la propiedad intelectual y el tratamiento de los incidentes informáticos.

Para el éxito de las recomendaciones jurídicas en materia de seguridad de la información es clave que las mismas estén alineadas con la estrategia y política general que el *Gobierno de Guatemala adopte en esta materia; porque 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 formule una organización.

Adicionalmente, la empresa de las compañías en diferentes sectores económicos implica el cumplimiento de una serie de disposiciones técnicas, 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 formule una organización puede ser el punto de encuentro de todas las disposiciones legales y reglamentos a que será sometida una organización en desarrollo de su actividad económica en diferentes países. Cuando la ley no existe o se presentan vacíos en su alcance, corresponde a la política de seguridad servir de guía a la organización en el cumplimiento de sus obligaciones, deberes o cargas. Esta situación ofrece un espacio interesante de autorregulación, en la medida que la organización podrá incorporar las mejores prácticas o estándares en una determinada materia; situación que por demás, facilitará el cumplimiento de la normatividad que deba acatar en diferentes países en los cuales tenga presencia, siempre

que las mismas no sean contradictorias. Adoptar un estándar o una práctica foránea, que no esté normada en un país, implica un cumplimiento más allá de la ley, lo cual en nada perjudica a la organización, sino, por el contrario, puede generar un beneficio importante tanto para ella como para sus grupos de interés. El reto para los encargados de proteger la información en una organización es 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 en cada organización seguramente habrá de ser diferente, pues la misma debe ser formulada sobre la base 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".[44]

Se debe garantizar la protección de los datos personales y la privacidad, de acuerdo al derecho a la intimidad de que gozan todas las personas; porque 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 tener, acudiendo para ello a programas de bases de datos, que terminan entregando información valiosa sobre los hábitos de consumo de un individuo.

[44] **Ibid.** Pág. 53.

Esta posibilidad de que terceros puedan acceder sin control a la información personal de un individuo es lo que busca proteger el derecho a la intimidad; 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 desconozcan esa tutela constitucional que cada individuo tiene sobre su información; así como sobre los perfiles diseñados a partir de sus hábitos, comportamientos y tendencias.

En consecuencia, en materia de seguridad de la información y para el desarrollo de este derecho fundamental, el Estado guatemalteco debe procurar que toda base de datos, tenga connotación comercial o no, cuente con las medidas jurídicas, tecnológicas y físicas que aseguren su protección; porque la ausencia de una norma que regule adecuadamente esa información, 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, variedad, 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; especialmente en aquellos casos de ejecución de proyectos

contratados con terceros no pueden dejar al margen la regulación contractual de las obligaciones que estos 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 éstas 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 se haga de los mismos; y en consecuencia, serán responsables de los perjuicios que irroguen a los individuos titulares de los datos personales. 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; puede ser garantizado a través de acciones de tutela, con el riesgo de indemnizar los perjuicios causados.

Para garantizar esta protección se ha desarrollo la seguridad informática, la cual es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con ésta; incluyendo la información contenida. La implementación de esta protección se realiza a través de una serie de estándares, protocolos, métodos, reglas y herramientas concebidas para minimizar los posibles riesgos a la infraestructura o a la información.

Los sistemas de seguridad surgen como respuesta a uno de los principales riesgos que afectan al desarrollo del acceso a contenidos en los nuevos medios digitales (internet,

comunicaciones móviles, televisión y acceso de banda ancha); esto es, la necesidad de ofrecer una adecuada protección de los derechos de propiedad intelectual de dichos contenidos; que a su vez sea compatible con el modelo de creación, acceso y uso de los mismos que se pretenda.

La seguridad informática comprende programas para computadoras, bases de datos, metadatos, archivos y todo lo que la organización valore y signifique un riesgo si ésta llega a manos de otras personas. Este tipo de información se conoce como información privilegiada o confidencial.

5.2. Medidas específicas para promover la seguridad informática

Utilizar internet para realizar transacciones económicas, tanto gestiones bancarias como pagos de comercio electrónico, aunque todavía no es algo muy habitual tanto en la actividad empresarial como en la de de los ciudadanos en su faceta de consumidores la tendencia en Guatemala es que la mayor parte de las actividades comerciales se orienten hacia estas dinámicas. Ante esta posibilidad, resulta fundamental seguir una serie de buenas prácticas y medidas para garantizar que todo el proceso se realice con seguridad, reforzando la confianza como usuarios de estos servicios.

Entre las principales medidas que se pueden aplicar para esta nueva forma de actividad productiva, se encuentra la autenticación para legitimar la identidad, los procedimientos para garantizar la seguridad durante el proceso y la promoción de buenas prácticas en

general, que incluyen consejos para hacer que los pagos en línea y operaciones bancarias se realicen de forma segura.

Las medidas de autenticación son un proceso mediante el cual se confirma que quien se conecta y solicita acceso a un servicio es realmente quien dice ser o sea, el legítimo usuario, para lo cual existen elementos tecnológicos, quienes son los principales encargados de autenticar el proceso desde su inicio tras la conexión con el servidor destino. La elección de unos u otros dependerá siempre de la infraestructura proporcionada por el comercio o banco electrónicos y las posibilidades de la conexión o dispositivo mediante el que se realice el proceso.

Hasta ahora, el elemento más utilizado para comprobar la legitimidad del usuario que solicita realizar la transacción ha sido el uso de claves de acceso. Existen multitud de mecanismos que se han ido mejorando y adoptando a lo largo de los años, tales como el pin o contraseña, puesto el número de identificación personal es la medida más sencilla y clásica de identificación, porque el banco o tienda en línea facilita una clave numérica o código alfanumérico para identificar al usuario, que deberá ser introducido en el formulario correspondiente en el momento de la autenticación.

Asimismo, se encuentra el número de autenticación de la transacción, la cual se trata de una evolución del pin, el mismo está formado por una lista o tabla de códigos que, en función de las circunstancias, pueden haber sido previamente generados y distribuidos de manera física a través de hojas de papel, tarjetas o distribuirse instantes antes de la transacción a través de medios digitales o dispositivos electrónicos. Su ventaja es que en

cada transacción, se solicita una clave distinta, siendo variedades de este procedimiento que antes de la transacción el banco envía el número de identificación a través del teléfono celular del cliente, en un mensajito, por ejemplo.

"Además, existen las denominadas captchas al proceso. Los captchas son imágenes con información en su interior que se supone solo podrán ser leídas por humanos y no por programas automatizados. El captchas mostrado puede identificar el número de identificación de la transacción a introducir o utilizarse como método de comprobación de identidad, mostrando por ejemplo la fecha de nacimiento del usuario".[45]

Puede crearse una contraseña de un solo uso, que trata de una clave de un solo uso, que generalmente es enviada por correo electrónico o mensaje de texto al teléfono celular y que también puede ser generada a través de dispositivos, dejando de ser efectivo en el momento en el que se realiza la transacción.

"Los Tokens son dispositivos electrónicos independientes o con conexión usb a un pc. Permiten generar claves privadas aleatorias según un patrón o mediante sincronización con un servidor externo. En un momento dado el banco solicita que se introduzca la clave de acceso generada por el token del cliente. Generalmente sólo se tendrá que activar un botón para que se calcule".[46]

Una de las medidas de seguridad más comunes, son las llamadas tarjetas inteligentes, las cuales son dispositivos de identificación del mismo tamaño que las tarjetas de crédito, que

---

[45] Observatorio de la Seguridad de la Información. **Medidas de seguridad online**, pág. 4.
[46] **Ibid.**

cuentan con un chip en el que guardan información. Muchas de las nuevas tarjetas de crédito son en realidad tarjetas inteligentes, lo cual les ha permitido en su elaboración abandonar progresivamente la obsoleta banda magnética para la identificación.

Este tipo de tarjetas necesitan lectores conectados al ordenador y permiten la identificación cuando el programa de computadora conectado en línea que se está utilizando lo necesite. Su potencial es la capacidad de albergar información privada dentro del chip y, dependiendo del tipo de chip utilizado, pueden ser reprogramados posteriormente para incorporar o actualizar los datos internos. Su principal función es guardar los certificados personales de usuario. Un ejemplo claro de tarjeta inteligente es la idea originada del Documento Personal de Identificación o DPI, en donde se pretende que tenga en su memoria toda la información del portador y la misma pueda actualizarse cada cinco años.

Por otro lado, existen los denominados dispositivos biométricos, los cuales se basan en una cualidad e incorporan el factor de autenticación; es decir, buscan una manera precisa e inequívoca de identificar al usuario utilizando para ello partes de su cuerpo, siendo los más usados los lectores de huellas dactilares, de la palma de la mano, de retina y los identificadores de voz.

Aunque puedan parecer dispositivos destinados a grandes empresas y organismos, en realidad están siendo adoptados a todos los niveles de forma gradual y ya existen iniciativas bancarias para implementarlo como medida principal de identificación de usuario.

Actualmente se están promoviendo también los certificados digitales o virtuales, como un elemento imprescindible para iniciar una conexión segura. Los mismos son archivos que identifican usuarios, empresas, organismos y, más comúnmente, la página a la que se accede. En resumen, se trata de una serie de datos personales unidos a una clave pública, y todo ello firmado por una entidad que les da validez, siendo este el objetivo de la creación de la Ley de Firmas Digitales, para que exista un registro oficial de las mismas y operadores que extiendan los certificados.

Los certificados se pueden utilizar a través de los navegadores, que utilizan los usuarios personales o corporativos, quienes los tienen instalados en el equipo cuando los necesitan. De igual manera pueden utilizarse a través de una tarjeta inteligente.

El certificado digital típico está compuesto por el nombre completo de la persona u organismo a identificar, el nombre de la autoridad certificadora, el número de serie y la firma digital del certificador.

La ventaja principal de estos certificados digitales es que resultan de una combinación de diferentes mecanismos y protocolos, tanto de los componentes físicos de la computadora, como de los programas que corren en la misma, que permiten realizar transacciones electrónicas con seguridad, basándose en la criptografía de clave pública. Actualmente el cifrado es el elemento conocido más adecuado para asegurar el proceso de principio a fin, garantizando la integridad y confidencialidad de la transacción.

El cifrado es la alteración de las comunicaciones de forma que se dificulte su comprensión por agentes no autorizados en caso de que puedan interceptarlas. Cualquier transacción en línea o digital debe estar cifrada criptográficamente, puesto que es el único método matemático que, si se realiza en ausencia de piratas informáticos u otros elementos distorsionadores, garantiza la seguridad de la operación.

Lo más importante de la implementación específica de estas medidas es que en la actualidad, tanto los comercios como los bancos que llevan a cabo sus transacciones electrónicas, cuentan con la tecnología para implementar las medidas de seguridad, así como con el respaldo tecnológico de instancias nacionales como los desarrolladores de programas computacionales de acuerdo a las necesidades de los clientes.

Se considera que la importancia jurídica de implementar medidas de seguridad en los medios digitales para transacciones electrónicas; radica en evitar que todas aquellas organizaciones sean vulnerables a que terceras personas sin autorización puedan tener acceso a toda información valiosa y privilegiada de las personas que confían en que sus datos personales no serán utilizados de manera inadecuada y que a la vez sean perjudicados en su patrimonio; que es una de las principales causas por la que la delincuencia organizada trata de ir adelante de la tecnología; fuente en la cual ven un negocio fácil de agenciarse de recursos económicos sin importar estratos sociales.

En consecuencia la seguridad jurídica precisa el estudio de la actuación de cada uno de los sujetos que intervienen en la transacción; a efecto de determinar a quién corresponde la responsabilidad en caso de fallos técnicos, violaciones a la privacidad, operaciones no

autorizadas o fraudulentas u otras transgresiones en el cumplimiento de los deberes impuestos por normas legales o contractuales.

Además, se puede indicar que los fraudes electrónicos se continuarán cometiendo en Guatemala, mientras no exista una legislación penal orientada a tipificar la mayor cantidad de ilícitos que se cometan a través de medios electrónicos; pues si bien cierto el actual Código Penal contempla desde mil novecientos noventa y seis los delitos informáticos, esto no es suficiente; siendo necesario que tanto los funcionarios del Ministerio Público como los juzgadores tengan una especialización en la materia; cosa que en la actualidad no existe, pues a todas luces se siguen cometiendo esta clase de ilícitos penales, en donde el principal afectado es el tarjetahabiente.

CONCLUSIONES

1. La informática jurídica ha sido un avance tecnológico de gran importancia para acelerar la información, los trámites y procedimientos en materia legal; sin embargo, su desarrollo e implementación en la mayoría de dependencias públicas y empresas privadas de Guatemala, todavía se encuentra rezagada en relación a su utilización en otros países.

2. El derecho informático como una nueva e importante rama jurídica, es el estudio y regulación de todas las actividades que se realizan utilizando una computadora; a pesar de ello en Guatemala todavía no existe una línea de investigación ni especialización sobre esta ciencia jurídica.

3. El comercio electrónico ha evolucionado de tal manera que representa a nivel mundial la actividad económica con mayor crecimiento, al extremo que las compañías más importantes tienen sus portales electrónicos para que sean visitados por los usuarios; lo cual no sucede en Guatemala, porque son pocas las empresas que usan este medio para sus negocios.

4. Así como ha crecido el uso de internet, también se ha incrementado la cantidad de delitos, como el fraude, en esta nueva modalidad de comunicación informática; ante lo cual otros países han especializado personal y tecnología para enfrentarlos, pero Guatemala, a puras penas ha comenzado con la tipificación de esos delitos pero carece de especialistas para perseguirlos.

5. Para lograr la consolidación del comercio electrónico, los Estados de otros países y las empresas bancarias han implementado medidas de seguridad que incluyen una constante información al usuario sobre las distintas formas de estafa electrónica; así como procedimientos para evitar que sus sistemas sean vulnerados, cosa que no sucede en Guatemala.

RECOMENDACIONES

1. La Secretaría General de Planificación –SEGEPLAN-, debe establecer un plan estratégico para que todas las dependencias públicas que tengan departamentos de asesoría jurídica, tengan implementados sus procesos a través de la informática jurídica; con lo cual se logrará que las mismas sean más eficientes y puedan conectarse para realizar un mejor trabajo.

2. Que el Colegio de Abogados y Notarios de Guatemala, promueva la creación de cursos libres y diplomados sobre derecho informático a sus colegiados; para que estos se actualicen en esta nueva disciplina y puedan adecuar su práctica de abogacía y la notarial en las nuevas orientaciones que esta ciencia establece, con lo cual pueden atender mejor a sus clientes.

3. Es necesario que la Cámara de Comercio de Guatemala, impulse cursos y capacitaciones sobre la importancia de que las empresas y empresarios individuales afiliados, desarrollen una línea de promoción de sus productos a través del comercio electrónico; con lo cual pueden llegar a más usuarios con menos gastos en publicidad, y hacer más negocios.

4. La Unidad de Capacitación del Ministerio Público, debe establecer un diplomado sobre fraudes por internet a los auxiliares, agentes y fiscales, para especializar en este tipo de ilícitos a los mejores; con lo cual se tendrá personal idóneo para llevar a cabo una persecución penal efectiva sobre las personas que se dediquen a este tipo de delitos penados por el Código Penal.

5. Que el Ministerio de Gobernación, conjuntamente con la Cámara de Comercio de Guatemala, establezcan una política para implementar medidas de seguridad en el comercio electrónico; que incluya una constante información al usuario sobre las distintas formas de estafa electrónica, así como procedimientos para evitar que sus sistemas sean vulnerados.

BIBLIOGRAFÍA

ACEDO QUEZADA, Octavio. **Temas y problemas que la informática ocasiona en la formación del consentimiento contractual.** México: Ed. Ariel, 2004.

ALADI-Secretaría General. **Situación actual y perspectivas del comercio electrónico en la región.** Chile: Ed. Santana, 2006.

Apoyo Consultores. **El comercio electrónico en Perú.** Perú: Ed. El Sol, 1998.

ARIAS DE RINCÓN, Mauro. **La protección al consumidor en el comercio electrónico.** Argentina: Ed. del Águila, 2003.

BIELSA, Rafael. **Informática y derecho: aportes de doctrina internacional.** México: Ed. La Ceiba, 2001.

BUENO CAMPOS, Enrique Rafael. **La banca del futuro. Un desafío para el 2050.** México: Ed. Siglo XXI, 2006.

DAVARA RODRÍGUEZ, Miguel Ángel. **El documento electrónico.** Chile: Ed. Antártida, 2008.

ESTEBAN, Francisco Javier. **La sociedad de la información electrónica.** México: Ed. Fondo de Cultura Económica, 2006.

FALCON, Enrique. **¿Qué es la informática jurídica?: del ábaco al derecho informático.** Argentina: Ed. El Malecón, 1999

HERNANDO, Isabel. **Seguridad y fiabilidad en el comercio electrónico: autoridades de certificación.** México. Ed. Universidad de Michoacán, 2005.

INZA, Juan. **Comercio electrónico. Cómo deben prepararse las entidades financieras.** España: Ed. Tirant lo Blanc, 2001.

MÁRQUEZ, José Fernando. **Elementos de la contratación electrónica.** Argentina: Ed. Jurídica, 2004.

MARTÍN PEÑA, Ricardo. **Exposición de una operación de comercio electrónico seguro con una tarjeta bancaria.** México: Ed. Universidad Nacional Autónoma de México, 2005.

MARTINO, Antonio. **Sistemas expertos legales.** México: Ed. Universidad de Michoacán, 2001.

NOVOA MONREAL, Eduardo. **Derecho a la vida privada y libertad de información: un conflicto de derechos.** México: Ed. Mc Graw-Hill, 2003.

NUÑEZ PONCE, Julio. **Derecho informático.** México: Ed. Fondo de Cultura Económica, 2001.

OBSERVATORIO DE LA SEGURIDAD DE LA INFORMACION. **Medidas de seguridad online.** España: Ed. El Tiempo. 2003.

PARDINI, Aníbal. **Derecho de internet.** Argentina: Ed. Jurídica, 2000.

SAINZ DE VICUÑA, José María. **La distribución comercial: opciones estratégicas.** México: Ed. Del Ángel, 2001.

Legislación:

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

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

Código de Comercio. Decreto número 2-70 del Congreso de la República de Guatemala, 1970.

Ley de Protección al Consumidor y Usuario. Decreto número 06-2003 del Congreso de la República. Guatemala, 2003.

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